ETHICS OF RISK MANAGEMENT

IN A GROUND-BREAKING INDUSTRY

Apocalyptic risk event philosophies will impede advocated theories, illuminating the factual results of controls failing at the hand of psychology emanating from humanity.

By: Albert C van der Vyver

Prologue

The book is written by a practitioner, advisor, and risk owner with a practical perspective rather than an academic interpretation of risk management. That makes it more interesting, as it is based on experience crafted between obligation and guilt, retained over many years as an employee, supervisor, manager, and consultant in the mining industry.

Observation shows that the mining industry strives towards a resilient risk management process, mounting philosophies of excellence in all matters of zero harm. However, undertaking such a pathway and climbing the maturity ladder gives rise to risk and exposes managers' volatility. Understandably, within the devious and unpredictable endeavours lies the change-hostility of the maturity process. First, observing the industry's system flaws would be best to exemplify this somewhat illusive matter.

- Perceptively, many managers and consultants went through plausible risk avoidance crusades, developing contingency and recovery plans that showed the resilience of their systems. Most of these programmes were developed essentially focusing on “proof after event”. In other words, a dam wall fails, and plans are in place to recover. The expectation is that resilience exhibits the control perception. Many of these plans are generic in execution, and few are simulated in effect. During assessment, the eye of the beholder is used as consent to the level and detail of control. To augment this notion, a company will have pre-condition risk assessments indicating risk owners' vulnerability. They will have well-developed risk response and contingency plans backed by strategies to get back to regular operation to articulate stakeholder confidence and maintain interest.
- These plans developed as a recoil after the event replicate the preceding state and denote the risk owner’s vulnerability with no real change. They are in

vain. They do not address susceptibility to risk. They never have and were never aligned to produce any other outcome.

- Risk prevention that neglects risk vulnerability is unsuccessful. It is dejectedly compelled by a harshly regulated legislator who does not concede risk management's realities and continually motivates risk reduction strategies through risk matrix number games.

Risk management programmes in the industry ought to transform and adapt to our challenging environment. The projected metamorphosis entails a matured risk framework that identifies, reacts to, and perpetuates vulnerability. Proactive systems do not mean identifying risk before the event; instead, they focus on identifying vulnerability and the control mechanisms to deal with it. Take a step to the left and prevent triggers of pre-conditions before the event, which proves to be more successful.

Content

History and Context of Risk Management

Linear overview

Many an author, including myself, who undertook the journey to the origin of risk management unearthed boundless disappointment. Reading through the well-documented research concluded by renowned specialists fabricated a broad spectrum of interpretations, each with a different timeline. The first hitch arises with the term risk management; we argue the origin of the English word, shift the timeline of history, or start to look at other words, such as probability of an event, all in vain. Ultimately, you will form part of a biased group of logicians. We have lost the fundamental rationale for risk by questioning historical evidence. Reasoning the opinion that probability analysis was the touchstone of risk management might be objectionable and reflect the view of a single group of dogmatic academics. Risk is not purely opportunity nor only about probability, and it contains an array of facets in testimony that risk management was evident even before or during the building of Noah's Ark. Biblically speaking, it has been with us since the beginning of time. People were constantly weighing up the outcomes of decisions; think again about what happened in the Garden of Eden, the fruit from an identified tree, and the snake. Was the decision not risk-based? Was uncertainty of the outcome present? Was this not the start of today's discipline, risk management?

Down the line of history was divergence formulated by anticipation and the endeavour to manage uncertainty. The political and social confrontation between countries has forever been opportunity-based, questioning what we can gain against what is at stake. As far as history was documented, evidence is significant in how inhabitants protect their cities from invasion. Such measures comprised sophisticated and well-deployed methods to offend the lust for rivalry. Exceptional projection and deployment of control mechanisms were demonstrated during ancient offensive strategies. The anxiety of having the correct prediction

of the next day, next week, or near future affected people with the vision to become rovers. Nomads formed new clans, languages, political views, and a new future for their followers. A true reflection of this day and age, we still have classifiable cults, trailblazers, and catalysts in each risk management discipline.

The construction of the Egyptian pyramids is an example of how risk-managing principles developed into a more mature approach. Many hypotheses were formulated over time, and various disagreements were on the subject. However, several facts must be addressed. Did they make use of migrant workers? What was the culture of the labour force? What was the weight of the stones? What was the impact of the weather conditions? Was stability of the structure anticipated, etc? All these questions are typically risk-based and should have formed part of the design and execution of the task.

During the High Middle Ages, which began after AD 1000, the population of Europe increased significantly as technological and agricultural innovations allowed trade to flourish, and the Medieval Warm Period climate change increased crop yields. Organising peasants into villages that owed rent and labour services to the nobles and the political structure whereby knights and lower-status nobles owed military service to their overlords in return for the right to rent from lands and manors were two ways society was organised in the High Middle Ages.

The Crusades first preached in 1095, were military attempts by Western European Christians to regain control of the Middle Eastern Holy Land. Kings became the heads of centralised nation-states, reducing crime and violence. Intellectual life was marked by scholasticism, a philosophy that emphasised joining faith to reason, and by the founding of universities.

During the later Roman Empire, the principal military developments were attempts to create an effective cavalry force and the continued development of highly specialised types of troops. The creation of heavily armoured cataphract-type soldiers as cavalry was an essential feature of the 5th-century Roman military. The various invading tribes had differing emphases on types of soldiers, ranging from the primarily infantry Anglo-Saxon invaders of Britain to the Vandals and Visigoths, who had a high proportion of cavalry in their armies. During the early invasion period, the stirrup had not been introduced into warfare, which limited the usefulness of cavalry as shock troops because it was impossible to put the full force of the horse and rider behind blows struck by the rider. The most significant change in military affairs during the invasion period was adopting the Hunnic composite bow instead of the earlier and weaker Scythian composite bow. Another development was the increasing use of long swords and the progressive replacement of scale armour by mail and lamellar armour.

The aforesaid is a summary of ancient history as a testimony to the persistence of humanity to develop an “all fits all” philosophy, which would indicate the end of the “defence mechanism” progression. Uncertainty about the effectiveness of these barriers arose with each encounter. New threats were recognised with each aftermath, eliciting amending tactics. This drive towards control improvement has channelled the industry to a submission ritual similar to what is central to a “cult”, with many followers in and outside the company at different hierarchies. Nothing has changed, and nothing will change at the end of time. This rivalry is printed in the human mind and is part of the realism philosophy.

Realism theory is the belief that many or most cognitive biases are not "errors" but instead logical and practical reasoning methods for dealing with the real world. The practical information people use in their reasoning process includes (but is not limited to) memories of things said by other people, people lying, people making errors, things changing, and that more time results in more changes.

Moving to a distinctive, relatively new intellectual tradition, enterprise risk management, the delineation is reformed, and the observations documented by most risk management authors reflect modern principles designed in the millennium of industrialisation. It would be factually inappropriate to portray only one side of risk management and neglect the others.

Take care. History does not govern risk, despite the academic value of its origin; it belongs to the past. It is unfortunate that risk managers still use historical information to establish the direction of the future.

Although we have used the words danger, threat, and risk interchangeably, the effect of misinterpretation should be alienated. Danger has its roots in the Anglo-French word *daunger*, which can be translated to the power to harm. The threat was first recorded before 900 and translated to the Middle English noun threat *(e)*. Risk originated in the 16's from the French word risqué and transformed into the English language in 1728. However, the commercial sense of risk was already captured in 1719 with the loss of material subjects. Thus, it is commercially recorded as a chance of losing something. The literature revealed that the activities of taking chances with games were formerly depicted in Egyptian tomb paintings from 3500 B.C.E. It was only after the numbering system was developed that calculations could simulate the opportunity. Douglas Harper, *Etymology Dictionary*, Online, updated on June 25, 2018, viewed 8 September 2022, https://www.etymonline.com/word/danger.

Undoubtedly, the best-defined timeline of the modern development of risk management can be found in the publication by Felix Kloman, a Fellow of the Institute of Risk Management (London). Reading through the Chapter of the publication, one must recognise the following.

> *"Perhaps Peter Bernstein's Against the Gods is a fitting end to this list of risk management milestones. It illustrates the importance of communication. Too often,*

new ideas have been unnecessarily restricted to the cognoscenti. Arcane mathematics, academic prose, and the secretiveness of current risk management "guilds," each protecting their own turf, discourage needed interdisciplinary discussion. Peter's lucid prose, compelling syntheses of difficult concepts, personal portraits of creative people, and particularly his warnings of the perils of excess quantification, bring us an appreciation of both the potential and perils of risk management. No matter what title we attach to this thinking process (risk management; enterprise risk management; strategic risk management; etc.), it will continue to be a part of the human experience."

-H. Felix Kloman*, A Brief History of Risk Management, Chapter 2,* President, Seawrack Press Inc. August 20, 2009

Georges Dionne, Professor of Finance and Chairholder, Canada Research Chair in Risk Management, has it and with respective references to sources of information that the risk management study only began after World War II.

- Georges Dionne *Risk management: History, definition and critique, page 2, 6* September 2013

It also goes hand in hand with industrialisation after the war when techniques were developed to improve the effectiveness and efficiency of process and manufacturing plants. Noticeably, most of the methods listed in the ISO 31010 originated during this period. Understanding the context of the origin of historical risk management concepts and how they progressed into a modern enterprise risk management framework is essential for the profession. Risk management is a skilled profession believed to be renowned as such. Risk managers of the future must prepare themselves for sophisticated risk analysis in all aspects of risk management.

Metamorphosis of risk management

Transmissible inherited mutation of risk transpired over many years. For one thing, in facing the risk of antiquity, people contended under humanitarian and social constraints directly influenced by the uncertainty of life. This strengthened the response to how humans could instinctively find a passage between facing danger compelled by the relentless drive of retribution towards the new aged, a matured defence mechanism of enterprise risk management. Unconsciously, we developed a few new phenomena during this progression. Revealed in many aftermath investigations that have followed man-made disasters, the cult of blaming and the cult of compliance surfaced. We not only invented the different avatars but refined them to become undetachable solutions to complications we failed to manage before things went wrong.

The opposite emerged from the dust clouds of blaming; we praise when opportunities are taken with consequential advantage. Notably, one should have anticipated that another cult would be on its way using the exact instinctive character mechanisms used in the past. Opportunities come with risk, and the cult of manipulating resources to influence outcomes and prove them wrong has right entered the boardroom. Playing games with the cults of blaming, compliance, manipulation, and the many more avatars that can be disclosed in the future is the most dangerous game. It is death-defying, and the livelihood of people can be destroyed in a single moment during a disaster.

The human brain is at the heart of historical mutation and deals with uncertainty. We all can agree that it is quite a fascinating organ. Without going into detail, specialists such as industrial, forensic, and criminal psychologists have studied how people behave, think, and act on matters that influence their cognition and emotions. Countless neurology studies have been done and are still underway to understand the mind and matter of the brain, which influence decisions and the allied cognition phenomena. The complexity of the brain function

is a maze, and comprehension exists in a reductionist stance, flouting density into small particulates. Prepositionally challenged and overwelled with the context, we acknowledge that risk management neglected the science of the mind and what indeed influences people to make difficult decisions. Soliciting the relevance of the said perspectives unveils an exciting interplay between risk culture in the boardroom and the scientific blueprint of neuroscience. Neuroscience is directly associated with behaviour science, which is interrelated with neuroeconomics and decision theory. Thus, metamorphically, we have proven that risk management is a science that cannot be based on people's perceptions, opinions, or reason.

Although some academics will differ in opinion or reason, risk homeostasis is a hypothesis, not a theory. An untested deviation naturally occurs in the brain to uphold inborn stability. When people negotiate with risk, they adapt to the surrounding influences to opt for the best outcome they perceive. In a boardroom, workplace, enterprise, or operational setting, they will base their decisions on their perception of the risk measured against an inborn target. People will modify decisions to eradicate any inconsistencies related to their acceptance of the norm of risk, thus signifying the influence of behaviour on decision-making. If a person involuntarily adjusts to the wrong direction, they will affect the outcome by alternative methods to re-establish the brain’s thinking process equilibrium. Risk homoeostasis offsets can become part of the analyses of root causes or trigger events towards risk, though more research is required to reveal the value of established effectiveness criteria. What is essential about risk homeostasis is that it should be the alternative methodology in managing what is generally denoted as behaviour or attitude.

Allocable legislation is the modern marvel of setting guidelines and monitoring regimes for managing risk. With little to no effect, it has subsidised a fabricated security consciousness. Let’s use safety as an example: The amount of safety legislation has placed the worker on a pedestal where they cannot use their initiative to ensure their safety.

Legislation even gave them the right to refuse to work, which is opposed by incentives. Countless regulations, subsequent Codes of Practice, and alternative Standard Procedures are all promulgated to protect the employee. No stone is left unturned during an investigation; the bottom line is that someone broke a rule, climbed the fence, and, for that reason, can be blamed. In essence, the objectives of safety legislation have deviated from the fundamentals of risk management. More time was given to investigations and aftermath punitive systems than risk assessments. How many statutory stakeholders participate in risk assessments? Notwithstanding those above, we have a place for legislation, and employers and employees have a pivotal role in adhering to these requirements.

The fence line during COVID-19 was more evident when the pandemic hit the shores of countries outside of China. Immediately, legislation, lockdowns and many more forced constraints to impede the movement of people were brutally enforced, and people were jailed or fined. The reality was that perception-based strategies initiated by weak data became the norm. Academically incorrect, but on the ground, people lived in shacks, up to ten in one house, with movement between homes one to two meters apart, overwhelming the control strategy. The control comes through awareness, and the subsequent homeostasis is affected by the numbers and visuals of dead people, which are communicated through different media platforms. Appalling is the fact that risk management principles initially applied made way for the legislator to govern the event, which left an aftertaste. The thing is that good risk response strategies are a set of pre-developed actions based on proven statistical analysis with defined trigger points enabling effective management of significant events. Interpreting what was just said, pre-developed means before the event takes place, but after identifying the possibility of such an event, not after the event has been initiated and then identified as a threat to a nation. Risk management is anticipating events rather than populating the history of known events. Take a closer look at your risk assessment and analysis of your company or

entity. Does it portray history or display future events that have yet to take place? Does the process indicate when to expect the event to take place (risk velocity measures)? Does it show preventive and mitigating measures and their effectiveness based on approved criteria? Metaphorically approved with perception through legislation.

Our social structures do not allow for large-scale pandemic control. Similarly, the existing work ethics and risk culture need to allow large-scale legislative control of risk in the workplace. The phenomenon of risk homeostasis embeds a paradox of inconsistency that readily aligns with the 'fence paradox' explained by Pasquale Cirillo, *Of risk, fences, and unavoidable falls*, 5 May 2018. When people are placed in an at-risk situation where failure is probable, they will be challenged by their minds to take the risk. Even if they fail the first time, they will negotiate another and yet another. It is, however, part of the game to fail and learn. These occurrences of failure are replicated by accidents in the workplace, which the legislators, stakeholders and authorities don't want. They then create fences through regulations, directives and workplace stoppages, forcing action into their way of managing risk. However, they generate an enigma where people's risk perception is modified. They underestimate risk. Risk homeostasis: Does the modification subconsciously lead to catastrophic consequences when multiple people are affected by the failure of the fence? Labelling the industry for the outcome as dangerous, poorly managed, and having a weak risk culture. This is ill of nature and indicates the failure to take the obligation of weak legislative requirements.

The problem is that we still believe we live in extraordinary times. Life is complicated, and the economy is in a spiral. War is at the doorstep, mining is dangerous, etc. This fallacy of thinking is pessimistic and causes increased pressure on the owner. Today's societies have become obsessed with success and will do everything to obtain status, even if we must change our norms and values. Politicians will go on a rampage of defaulting each

other and fraudulently become the new reign in the country. We have become so used to the way of doing that it has become the local norm. Risk events in a procurement department are no longer reported; they are never investigated or taken action until someone rings the bell. Even then, the person who blows the whistle is taken out of society, metaphorically, because they act 'against the norm'.

Extraordinary times create situations where executives, like the legislator, suspend, amend, propose, and approve new constraints to fence the problems. This 'state of exception' that the fence is the correct line is lost in the face of disaster. When a tailing dam wall fails, we suddenly feel bewildered and anxious and lose our historical reference point. Where was the legislator who designed and monitored compliance with the preventive controls? Similarly, where were the executives, the owners, and stakeholders? The same political pressure of success, along with investors who do not understand the material risk linked to the monetary risk, is based on events impacting the livelihood of workers and the local communities. Obligation comes through empathy, and the moral obligation to protect fellow workers and others should have been a part of the culture before the disaster. When local government and authorities deal with possible threats reported to them, they should appoint expertise to provide the necessary risk management guidance. Still, instead, they use a radical bloodbath approach. The more finger-pointing and blaming, the more they become confident, and communities thrive on these statements. Regrettably, the risk stays the same, and it will be confirmed and cause extensive damage to infrastructure when the dam wall fails.

Unfortunately, we risk forsaking our authorisation and discretion to manage risk. The legislator's invasion of an in-loco investigation creates an opportunity to grant the affected community a feeling of power and safety. A statement that the owners will be held responsible has become common during these visits by authorities. To find the actual courses, they will overturn each stone, paper, and dustbin to see how this could have happened, what

has triggered the event defence mechanisms to fail, and how they can strengthen the fence. In the aftermath of the tailing dam wall failure, people will be prosecuted, new controls imposed, more pressure on owners and lastly, people will 'feel safe' again, same as before the event, they are not! Even with the best technology, we endeavour to prevent risk, even if it is impossible. We start to become irrational and reckless in our effort to maximise profit and build fences of protection.

Metaphorically, they and their regulations have become problematic in managing the risk of the new era of technology and the incoming fourth industrial revolution. Legislation aimed at directing and controlling risk within an industry that rapidly reacts to change will be history by the time it is promulgated, ineffective and, in some cases, enlightens the burden. Legislation is no longer a cure but a constituent of systemic risk to the industry and the legislature. How do we manage risk? Concisely and practically, we identify the risk, evaluate the impact, and set up controls to monitor. How does the legislator develop regulations? Again, practically, they wait for an event, investigate, change, or introduce regulations. One more proactive than the other. As risk specialists, we have failed our profession if we accept that regulations govern risk. We will prepare for another catastrophic event if we do not assume that risk is evident and unavoidable. We can use mathematical calculations and simulations to mitigate risk and understand the nature of exitance, but the subject remains our human intervention. Many managers have generated risk assessments that denote goal-directed control activities, often reasoning experiences that modify the original motivation of the risk acceptance strategy and alter unintentional outcomes to be lesser. We should take care of modelling risks and use our common sense.

More examples might shed light on the issue of fencing off by legislation. Spring-applied hydraulic release brakes were legislated for vehicles that operate in the mining environment. Yet they can and will fail, with or without a risk assessment. Operators have

become complacent that the brakes will always work and protect them from a runaway vehicle, they feel safe. Not so, it will fail by design under several circumstances. Manufacturers and Engineers accept the risk, and the legislator is content with the situation. Until the accident, then through investigation, we imply that human error was the event's root cause. A fire in an underground coal mine is regarded as the most significant event for coal mining.

Let’s put the exact vehicle to the test. We employ a fire suppression system on the car with an automated initiation device activated by temperature increase, releasing an extinguishing medium directed to the point of the fire through a nozzle. Who decides where to place these nozzles? The fire specialist? What is his knowledge about a vehicle and where the fire will start?

It will most likely be directed to the engine compartment and electrical systems. However, the heat generated in the brakes transfers to the wheel assembly and may result in a fire of the hydraulic fluid. After a fire, the investigation will reveal that the nozzles were placed in the wrong position. Thus, by design, we have accepted a risk that is evident to happen; it is waiting for the right circumstances, and in most cases, when the catastrophic event is not expected. We had a few conveyances that fell down a shaft. We never expected it to happen again after the Vaal Reefs disaster, but it did, and almost every year, a similar event occurs. Because no personal injury was involved, we cannot neglect that we work with an unacceptable risk governed by legislation. Do we need to learn, change the controls, set up more defences, and add legislation to define weaknesses in our risk management systems virtuously?

Transformation is apparent; the way human society functions develops over time, and the setting of new social structures becomes more dynamic. Human conduct, its causes and consequences relate to the transformation processes that preserve and change them.

Characteristics of transformation are two embedded risk factors: uncertainty and ignorant perceived outcomes. Metamorphosis subverts the risk factors in the face of the prevailing world. Catastrophic risk events are professed as unintended, unthinkable, unrealistic, and go past unnoticed. Ulrich Beck, a renowned German sociologist and one of the most cited social scientists in the world, noted that the theory of metamorphosis is not about the side effects of the good but the positive impact of the bad. Risk professionals are leading the practice of analysing possible outcomes and recognising the potential good that can be exploited to change the future.

Changing the nature of risk

'Risk and time are opposite sides of the same coin, for if there were no tomorrow, there would be no risk. Time transforms risk, and the time horizon shapes the nature of risk: the future is the playing field.' *Peter Bernstein, Against the Gods, John Wiley & Sons, New York,1996 (Revision September 2008. An earlier version of this brief history appeared in the December 1999 issue of Risk Management Reports.)*

Companies' commercial and operational environment has changed and will forever change as new technology comes to the front. We live in a fast-paced industrial world, and the 4th industrial revolution created a challenging milieu for risk managers. Those who have assessed the velocity of emerging risk have already upskilled their systems and prepared themselves to conceive the new. Those who are left behind will take action on their effects and fall into a spiral of deceived practices. Transformation becomes more necessary on the day as the demand to increase efficiency and accommodate labour obliges intensify.

Besides continued market volatility, Governments and stakeholders worldwide are looking to reduce costs and secure sustainable revenue. We must develop and maintain a new series of programmes for risk professionals that will propel a critical eye on enflaming risks well into the future.

Sculpted to be provocative, alluded practices projected for the future by risk professionals are embryotic by nature. They are new and have yet to prove the elderly wrong; as long as wrong is not wrong, the right cannot be correct principles are followed in the operational arena. Habitually deserted because of their nature, and people thrive on this principle; it gives horsepower to their single-mindedness until the big one hits the media. We must embrace the sources of advice and cultivate a culture of understanding for the new. Research done over the past few decades by international organisations such as the Institute of Risk Management should be taken to heart. One of the latest surveys published in the Winter 2021 Enterprise Risk, an official publication of the Institute of Risk Management (IRM), implied that only fifty-one per cent of businesses are fostering risk culture.

On the other hand, we have close to eighty per cent of investors prepared to capitalise on companies willing to increase their Environmental, Social and Governance (ESG) performance. Owing a risk culture creates strategic relevance where investors continually escalate their focus on ESG and political stability. Companies can only survive the withdrawal of investors; similar can be said of investors; only some can survive without investing with companies that pursue opportunity. Many doors have opened and closed during the period of liquifying economies, political disturbances, and confrontations. Opportunities are the future of risk, inhabited by the advice and design system revolving around enduring the nature of risk.

These early stages of changing horizons will keep risk managers awake for a long time. Not only do they have to become more professional in their conduct, but they will also have to be educated about the emerging knowledge of the time. If risk is intensifying its change, we need to examine the factors that compose it.

- Second-hand experience is antique – Risk has passed the point of yesterday in time, in control and response. The influence that the alleged experience has on

risk assessments is as old as the experience itself. Timeworn understanding is not required, and more, copying and pasting information from one risk assessment to another, from one data source to another and filtering what is needed to claim due care is ill and does not belong to the profession. Remove all second-hand information and reveal the fundamental nature of the risk and its exposure. Stakeholders must understand the concepts and be informed of the consequences of using time-past information. They will require redundancy built into the system, allowing them to make timely decisions, alleviating the consequences, and avoiding future surprises.

- Fragmented risk appraisals are non-functional – The concentrated focus on emerging risk that is not integrated closes windows for opportunities. A holistic approach is required, as we have experienced in the International Standard Organisation guidelines for risk management and the implementation philosophies of the Institute of Risk Management. Fighting fires in the aftermath of significant events is fragmented intellectual property. Typical examples are the immense effort put into mitigating controls after a major disaster, all focus changes to the preceding event, and the future being neglected for a time. A well-defined cradle for the birth of risk migration, we will awake when the next event happens on unexpected grounds.
  Deceitful information disseminated to stakeholders affecting and diverting the allocation of resources from the current and actual risk is the source of the next event. This happens when priorities change and become a personal matter, detached from company objectives. Toxic managers have a predisposition to recast emphasis, purposefully or subconsciously, to align with personal intents, which enables them to mask their insecure abilities to

manage risk. Invasive expenditures follow these managers, which will fragment the realm of risk and have no efficacy or meaning.

All executives and managers will undergo one or more downscaling and upscaling processes during their work life cycle. It then does happen that positions are redefined and reallocated. Over time, experience proves that the so-called ‘soft skills’ and ‘non-core’ services are mostly exposed to downscaling. When upscaling and engaging resources become a poaching exercise, cost is not spared for core business positions. The risk manager falls in the non-core position and has been in this category since the beginning. Dejectedly, we have seen that lateral movements are made to retain a person's knowledge and skills. So, has an engineer or production manager been laterally moved into the risk management position, knowing that the position requires a designated proficiency to realise the company's risk objectives? Up or downscaling operations has been a challenge for all the years, mainly because of the poor risk management strategy that was followed before the implementation, which leads to disintegrated job specifications, which, on its own, produces more risk to the company objectives.

Outsourcing expertise requires a firm evaluation of service providers' capabilities, efficiency, and efficacy and how they integrate with the company objectives, risk culture, and risk appetite. Service providers that provide a professional service will generally have professional indemnity insurance. Their advice is used to manage risk, the risk real, and who is to wash their hands in water, the service provider. The attempt to sub-divide or, in risk management terms, transfer the risk of liability might not stand in a court of law. Fragmentation of accountability and liability becomes non-functional in

the face of the public when many lives have been sacrificed or people's livelihoods are at peril.

A water use licence cannot govern the risk of a tailing dam wall failure, whether a water storage dam, dirty water dam, or run-off water dam. Structural integrity is at risk and compromised. Trigger mechanisms differ for each structure and require expertise to evaluate the effectiveness of controls. When the water use license was issued, it was not done in aggregation with a risk assessment of the dam wall integrity control. The person(s) who approve the water use license has no expertise in structural integrity and dam wall construction. Refrain from fragmentation of controls during the aggregation process the risk. This is not a subject of control; it is a question of understanding the actual risk; fragmentation will create the fallacy that the risk is under control and will not be real unexpectedly.

Resilience does not signify the management of a singular or fragmented manifest of risk but being operationally equipped for anything. Disasters may come from unexpected success (leading to a constant decline in loss-time injuries entrenching a fabricated consciousness of safety) as much as destructive unanticipated failure (be that a workplace fatality, dam wall failure, total outage of communication systems, or large-scale fraud). Resilience systems are dynamic and show capabilities of rebounding rapidly to the norm.

- Augmented risk is a balloon to bust – Factors we deal with include the ‘number game’, the deliberate alteration of systems and the ignorance of indicators. Firstly, the industry has a deep-rooted culture to prove that what we do is right, and we are legally obliged to do so. Thus, operationally, we must

do a risk assessment to confirm it is safe to continue with work, which is imprudent. The objective was to manage the risk, not to show a lower number by the perception of a few. The number game has subjugated the risk assessment process of the South African mining industry since the mid-90s. Indeed, this was an Enterprise risk management principle where semi-quantitative risk evaluations and simulations were done, and some believed it might work in the operational environment. Well, it did not; it has instead caused confusion and confession. The latter took years of failure before the beholders recognised that it was toxic in delivery. Operational risk assessments in the industry affect the physical risk aspects of the organisation. Although overtone to negative effect, it remains a management function signifying due care, and not that the risk from a subjective matrix is lower after a few controls have been recorded with no defined effectiveness.

The same would apply to managing the oscillation of the factors that influence a specific commodity price. Hedging is an old game dealing with some key factors and their onslaught on business objectives; however, within the same factors are the grasslands for opportunities. Amongst them is affirming effectiveness maturity based on an approved and appropriate criterion. Avoid the subjectivity that augments the perception that all is well. Drive towards matured and distinct risk anticipation and response platforms.

Deliberate alteration of risk levels and control effectiveness by risk and control owners blatantly ignorant of the advice given by risk professionals has been captured in event data. In retrospect, these deliberate deviances will become silent evidence during investigations. Managers must take care and understand the impact of the decision-making process within the risk

management framework. Augmented decision-making converts into dysfunctional “Groupthink”, a psychological phenomenon followed by disaster.

- Mimic risk surveillance is an avatar in nature – Simplified, imitating risk control monitoring is personification in nature. One can observe risk maturity trailing some individuals, while disaster events are not far behind. Recognising the importance of the individual’s ‘predisposition to risk’ and ‘personal ethics’ in shaping people’s attitudes provides a window into this novel Avatar. Every individual comes to an organisation with a perception of risk. People vary in habit, and this includes their predisposition towards risk. Psychological research identifies two specific mindsets that contribute to this. One is the extent to which people are either spontaneous and challenging understanding or organised, systematic, and compliant. Secondly, the extent to which people may be cautious, pessimistic, and anxious, or optimistic, resilient, and fearless, ultimately becoming reckless.

  Using personality assessment tools, one can measure one's predisposition to risk. Several psychometric tools can facilitate this.

  Organisations must pay attention to the ethical profile of those working in their business. Every individual comes with their own balance of moral values, which greatly influence the decisions they make on a day-to-day basis. Psychologists have it common for behaviour traits that lead up to an act to be identified. However, one aspect remains undisclosed, which is that they cannot isolate before or after the event, and that is the state of being predisposed, also referred to as susceptibility. This implies that some individuals are exposed to a disposing influence well before the opportunity to manifest itself. They have

inherent preferences or biases in doing things in a specific manner, making decisions influenced by the interaction of particular biological, psychological, or environmental factors. They will imitate controls, correctly or not, but for them, it is the correct way; what is more, they will stand by the decision as the events transpire around them; they do not recognise the intrinsic exception. At the senior management level, the balance of risk types significantly influences team dynamics. It affects the collective perception of risk, willingness to take risks, interpersonal perceptions, information sharing and decision-making. The lower echelon supervisors will mirror this culture and, ultimately, the workforce. The approaching epochs will be muddled with these perceptions inflicted by a society where our actions force us to eat or be eaten.

- Control heuristic is pessimistic – In psychology, we tend to overestimate the influence of our behaviour upon events. We reason that we have control over uncontrollable outcomes. Available evidence suggests that people have a personal bias to obtain the expected outcome they perceive, even if they need to transfer responsibility. The material outcome will supersede the intangible outcome. The decision-making process in our brain will select the rosier part of the outcome as correct. It will weigh the pros and cons before stimulating "action" to control. For example, if I had to walk 800 meters up a decline tunnel to isolate the power to work safely on a conveyor belt and prevent accidental start-up, I might reconsider; there should be an easier way of doing the work. Instead, we can drop not one but two pull-keys, which will also prevent the start-up as they must be reset before the conveyor starts. The control heuristic suggests that the latter will prevail. It also aligns with the susceptibility avatar.

Future risk professionals should be aware of illusional factors in developing control structures and encourage systems that inform managers of the impact of emotional decisions.

- Beehive risk clustering is commonly criminal. Accumulating information and placing it into a polygon, a two-dimensional system for risk analysis has numerous limitations and produces large-scale deviations. Flexibility in risk analysis programmes will provide for other dimensions that harm the event outcome and subsequent consequences. Grouping risk into a box reduces flexibility and the ability to change, alter, and adapt to risk indicators.

  The trigger mechanisms of a risk event mandate the understanding of the threats we anticipate for profitable operations and the hazards we use to do business with. The earlier we can control the timeline of the event, the more effectively we can alleviate impact by calculating risk velocity.

  Risk management software tends to use generic terminology in the assessment practice. More so those that were developed out of a need for more financial provision and technical contribution. The decision that quality software is too expensive and Excel produces the same results will be the downfall of any program. Every system provides advantages and disadvantages; one must accept that limitations produce risks and opportunities. But, to cluster risk into generic terms and outcomes for “making a system work” is sinful.

  Those who change the objective of a risk assessment technique to suit their control heuristic dilemma provoke illicit deeds. Pragmatic in nature, they force the risk owner to cluster the risk into a specific cell in the massive beehive of events, neglecting the change in the operational environment affecting the occurrence. No recognition is given to hazard drift, risk velocity or

disposition, which are stimuli to the event. Ultimately, all end up in coded risk practice posturing controls directed to prevent the event. This beehive of Excel analysis comes with limitations, and it will be far from good to justify that a "homemade" tool for Bow Tie Analysis in Excel can produce the same results as the worldwide recognised software version of the same technique.

Professional risk managers endeavour continuously to improve systems. Part of their proficiency is to negate stagnancy and persistently observe developing criteria to comprehend mitigation through practical analysis using approved methodologies. Lessons learned from past events have shown that systems evolve or cannot keep up with the promptness of evolving risk criteria, which, in turn, ascertain principles for risk maturity, analysis, and control mechanisms.

- Eccentrical risk response is imitative – Habitual and opinionated conducts have filtered into the risk management framework. Over time, it has become a habit to challenge and deviate, by perception, from conventional or accepted practices followed by extraordinary outcomes. The mining industry has created several default methodologies to conduct its risk assessments. Historically, these processes centre around events known to occur, nothing different than populating the industry's history. Very few, if any, of the risk methodologies embraced an opportunity or resilient event identification process.

  Event identification is a subject of its own and possibly the worst-developed system of the total risk management framework in the industry. Pay attention to the supernational insight that surfaces in hindsight. Took to the table the amount of research done after a significant event and the number of papers

delivered at conferences following these events. No qualifications were found for educated people with exceptional solutions when the risk assessment was done. The problem resides not only in the methodologies but also in the availability of human capital that centres around a few persons within an organisation.

Companies must identify risks, but before further action, they must conduct a human capital assessment. Determine the capability and capacity of existing staff to continue with the process. Do the available persons have the knowledge or access to information to understand the risk in all features? An example that came to mind was the assessment of "sinkholes" in the coal mining sector. The team required a professional Rock Engineer and a Geotechnical Manager who were exposed to these risks. Along came a Safety Manager and Emergency coordinator, who took the lead during the assessment, having all the controls already pre-assigned to events that had happened in the past. It was a synthetic reproduction of a research paper done by a master's degree student. We should take care of the magnitude of events we are dealing with. The risk assessment process does not start with past event analysis and controls. It should begin with the identification process. Identifying stakeholders, communication, scope, and criteria will set the scene for a practical risk assessment. The critical identification process evolved into an operational risk assessment only when the more mature professionals became involved. It became the breeding ground for further studies to understand the risk of sinkholes and their interaction with old 1922 mining activities and hot coal.

- The enigma of human behaviour is mystifying. The ability to argue a point of risk does not show proficiency in the matter; it shows the inability to synergise the approach to managing the risk. After-event investigations have proof of these inabilities and shortcomings when it comes to the appointment of risk management staff.

  What we deal with here is not the behaviour of persons involved in incidents but rather the behaviour of persons responsible for the risk management structure implementation. On the negative side, we have developed, by default, several professionals who can advocate over years of legal boldness. They will interrogate every "change" to their perception of risk, argue definitions, constantly oppose new or alternative methods with superficial statements and show no argument in pursuit of a synergetic outcome. It is a winner-takes-all principle that has so often proven to be a system weakness and of habits that have devolved to alarming levels.

  It continues further; managers also must implement and maintain risk structures. Should it be wise to say we have the same concern at this level? Over the year of involvement with managers, their ability to perceive risk and set control principles evolved substantially and may, in some areas, be more mature than the safety staff. The phenomenon may be because of the regulating responsibilities of safety staff and how it was implemented. However, if we read carefully between the lines, the safety staff who carry a legal appointment had a much more advice-giving obligation than regulating. The question immediately comes to mind: Has the industry equipped them with the capacity to perform their work, or do we appoint people who still need to perform on production?

- Dysfunctional illusions - Combining legal safety, health, environment, occupational risk, and risk into one department with one function head. This was something other than creating a department that would be dysfunctional by the illusion of generic and similar objectives. It is as far as we can get from the truth. Any professional working in the designated subjects will acknowledge that each profession is different and manifests in other practices with dissimilar purposes. An example would be asking a medical doctor to sit through a risk assessment on the building they use for occupational health care. Structural integrity, electricity, backup power supply and many more were never a medical subject. Having an Environmental specialist as head of the function changes focus and budgets in that direction. A medical doctor must report to a safety manager or an occupational hygienist. It just does not make sense; how have we allowed a department to fall apart over a decade and degrade some of its functions? If it was a trial, then it is time to terminate it; if someone thinks it is working, they have neglected the risk assessment that was supposed to be done two decades ago before the amalgamation of the functions. It has caused harm to the safety and risk profession to such an extent that the industry has misconceptions about the future of risk management. We changed the name of the position from risk officer to risk specialist without acknowledging the person's mispositioning. A specialist will have a professional qualification and belong to an approved professional body. Has it not become time to assess the capabilities of the risk management staff, or should we not divide the function into legal obligation and risk obligation? Perhaps by then, risk managers will have the capacity to provide advice from a

professional platform. Like any other professional, risk professionals subscribe to work ethics specified by their profession, such as engineers.

- Happenstances influence the perception of outcome - A remarkable coincidence that the concurrence of events or circumstances was simulated in a risk assessment without realising the apparent causal connection to vulnerability gives rise to a perception that we have attained objectives. However, in reality, it is merely a miscarriage of the integrity of a system. Examining the causal factors of risk means scrutinising the traits that motivate the actions leading up to an event. These engagements need to be added to the time we spend with risk assessments. Research has shown that events are a combination of factors that change in recognised factors, physical or immaterial, having a conspicuous demeanour on the perception of the magnitude of possible events. Having ulterior motives and a perception that the outcome of a risk assessment will provide for a management decision that specific action will reduce the level of risk to an acceptable level to justify the continuation of activities may have concealed disasters in design.
  Risk management's function is to cultivate a culture of understanding risk. Embedded in the function is donating time to uncertainty regarding the risk release mechanisms. Not only does this include the formulation of the magnitude that changes during the risk velocity during release, but also the misunderstanding of the effectiveness of our control framework. A mature control framework is directed at articulating, anticipating, and avoiding these antecedents and uncertainties.

In summary, we have to ask ourselves a number of questions to determine the impact risk management has had over the past few decades. Are risk management and resilience functions simply philosophies and mindsets? Is risk resilience a by-product of good leadership, or is it the other way around? Can we continue to blame behaviour as the source of all events?

Observation has shown that historical approaches were the foundation of injudicious decisions that produced catastrophic events in today's time. Historical data and analysis have proven useful when everything went well, but the same custodians scramble to derive proven risk prevention strategies when things go the other way. This phenomenon has confounded many companies in the wake of the disaster.

Our mining industry must further examine these matters to solicit business continuity. Resilience is a maturity bus word without an outcome, a mountain too high to climb and, in most cases, remains questionable on arrival. We can rename our approach, re-blame the source, re-do risk assessment, and increase work stoppages by the legislature. Still, the same principles ascend under the umbrella, upholding the same values. If the industry changes the direction of the existing philosophies, it will substantially impact education, budgets, and resources. The evolvement of risk management is evident, and mining companies must develop a culture of agility to alter roadmaps that will comprise defensive and offensive ingredients.

Mining and Risk Management

Since the start of risk management practices in the mining industry, we have shaped divergence about understanding “what we manage”, circulated by context, vulnerability, threat, and outcome. Pictures, videos, incident reconstruction simulations and advanced scanning are used to document and reconstruct an incident, detaining risk in real-time and simplifying the risk analysis process. Over the past few decades, we’ve been doing risk assessments in the mining industry, yet we battle to identify the root cause correctly. From experience, a clear line is drawn from a person's planning, instruction, observation, and failure. Notably, from control analysis, more than ninety-three per cent of all controls are administrative, requiring a person to do, act, and respond in a manner outlined in a procedure, standard, or rule. We have crippled the unfortunate workers, and things will go wrong.

In alleviating the problem, managers have recognised that the solution is not only about identifying the hazards. The problem is much deeper: understanding the way hazards materialise, the release or trigger mechanisms of the initiating event, and how hazards drift out of context or control and change their characteristics in a manner that is unrecognisable to the eye of the beholder.

“The mining industry is dangerous, ill-managed has a poor safety culture, and managers are careless”. A reverberating ancient and unpopular statement customarily made by uninformed people after every incident. Over time, these statements have annihilated innovation efforts by risk professionals and operational managers. I firmly want to believe that the individuals who made these populistic statements have the subject knowledge to voice such guff. I also confidently wish to think that they might become mindful over time. We must ascertain the dynamics that have shaped these intolerable and judgmental opinions.

- Embracing the service of risk professionals was but one of these evocative factors. Working in this profession does not proclaim the position of a

specialist; it is owned by designation, with experience, and registered by a professional body.

- The popularity of a system grows with a response. In other words, famous statements and slogans catch the eye, and everyone follows suit. An example might be the slogan Zero Harm. Very few know the background and the objective: it was a mindset rather than an objective outcome. The alarming focus on “silver bullets” (Critical Controls) has become a “cult” in our industry. Lagging indicators drive the popularity of a system; good accident records have been seen as an outcome of a sound management system. One success story becomes the carriage for the future, change is driven by disaster.
- The impact of risk culture and appetite. International research statistics published by the International Institute of Risk Management in the UK concluded a global survey indicating that less than 10% of companies have high-risk maturity, and approximately 60% have low-risk maturity. In the eyes of the public and policymakers, these studies represent the reason for failure.

Objectively, the mining industry, in all its aspects, attempts to prevent injury to a person; indeed, they will not deliberately cause injury; they are not criminals and should not be treated as such. I firmly believe that we have respect for our employees and employees for managers; when it comes to the lives of people, we do not play with numbers; humanity mandates the “no go” flag.

Incited by tragedy

Imperfect perfection represents how risk management evolved over the years and distinctively followed an ascending pathway to maturity fuelled by each disruptive event. Like cyclones, risk management is characterised by inward-spiralling events emanating from

pressure and change. Legal obligations, company risk appetite and industry objectives enacted the pressure. Where change correspondingly shadowed grievous events, the aftermath afflicts the need to alter course. This uncontrolled spiral effect has left a trail of catastrophic events within the mining industry, each revealing system improvement opportunities to increase risk maturity. A grave concern is that systems occasionally devolve like a cyclone that moves over land, weakening rapidly not just because of resistance to change but also because of overt or covert pressures amplified in pursuit of interim solutions.

The case: A 45-year-old man with bipolar disorder was working at a smelter operating a crane that moves ladles filled with 8 tons of molten metal. Like all other disasters, a combination of mishaps can be categorised by a significant sequence of smaller events that intensify the velocity towards the central vent. The crane driver of the next shift called in late; the crane driver was asked to extend his shift, and during this time, the full ladle was idling and formed a solid crust on top. The procedure was to move the ladle to a designated area where a rock drill operator would perform a risk-based procedure to remove the crust and pour the molten metal into an ingot. Because this was at the time of the start of a new shift, housekeeping was performed by the people who came onto the next shift. Water was used outside to wash off debris spilt over the night shift, leaving some water on the concrete floor outside the furnace building. Removing the crust was done using a rock drill. When the rock drill opened a hole in the crust, the hole crust fell out, allowing the molten metal to overflow the edge of the ladle tilted into position by the crane driver. Molten metal onto water equals rapid and violent explosion. The event was devastating, seriously injuring 13 employees, igniting an adjacent building and a veldt fire outside the premises more than 200 meters away from the explosion. The employees were all travelling past the activity, were not directly involved, and were unaware of the risk exposure in that area.

During the aftermath investigation, the focus was placed on the rock drill operator and his actions; remedial measures were like all the previous six events within the same activity: re-do the risk assessment, revise procedures, discipline the operator, retrain and enforce rules. Shift cycles were 12 hours for crane operators. Although the operator in question had a medical history, he was extended into a 16-hour shift for the second time within the same week. He was not injured during the event but became a silent witness to the tragic event. Unearthed was why this high-risk activity was designed and positioned in an area always filled with persons travelling to and from buildings or not in an enclosure.

Like all other root cause analyses, the investigation system was designed to find behaviour as a cause of any accident. It was only over time that we started to establish measures to evaluate the effectiveness of our risk management systems alongside the systems that validate the hazard competency of our people. We still battle putting a manager's mind into a worker's hands. Management sees hazards differently; the worker must recognise the deviants to the hazard from the stable to unstable condition, drifting or migrating from the normal and execute the task following a difficult-to-understand procedure. In this case, the reference to difficult means the complexity and level of language used to write these procedures. The industry has many persons with medical conditions that have yet to form part of our risk management strategies.

Many companies have designed risk-based decision processes that produce tragedies. As an example, the 12-hour shift cycle is a precarious decision. At some mines, employees must travel long distances to and from work. They form lift clubs to save on fuel. In my book, being on the road for an hour, coming to work for 12 hours, and then back home for another hour adds up to 14 hours, excluding time in the change house to prepare for work or leave the premises. What happens with family life? Then, to escalate the issue, the cycle is altered between day and night shift every month, or after three months. Disruption of the

brain cycles is appalling for fatigue management. The well-being programme is then designed and labelled to support the outcome of the shift cycle decision taken after a risk assessment, an excellent example of the industry's misuse of a risk assessment technique. Uninformed risk owners make use of default techniques to enforce already-designed decisions.

Disruptive risk management is the product of disaster management. History has disclosed that accident statistics have declined after each significant mining disaster. Graphs displayed with decades as intervals will support this notion. A rapid drop to almost zero followed each spike in the graph before it stabilised at the next lower level of acceptance. We cannot evolve our risk management framework and structures based on the outcome of disaster events. The industry needs to actively seek opportunities for improvement through proven strategies.

Inasmuch as we want our risk management system to be proactive, we inherently designed a strategy where our risk matrix has become a reactive tool. Companies that have shown a less matured risk management system have adopted a principle of “proofing” that risk control, mitigating and treatment have a numerical value to indicate effectiveness by lowering the risk level. Devoted to the process is the school that thinks residual risk is a number; sadly, they misinterpreted the guidelines and best practices. Risk per definition was never a number; instead, it evolved from the ISO 73 definition in the context of risk identification. For that purpose, it should combine the risk sources, events, their causes, and their potential consequences. One step forward: what entails residual risk? Then, the same, why would it be different? What is left after treatment? Describe the risk, not the number. Stakeholders are interested in the remaining risks after treatment, not those that show a decrease. The self-enacted adversity built into the system is that when the event happens, we very quickly ask ourselves, “Where did that come from?”. This is a fundamental principle of

risk management: do not play with the numbers unless a recognised quantitative study was done with simulations that show a decrease; no change should take place based on the perception of a person or a group of people.

The aforesaid should be noted as one of our industry's biggest missteps since 1996 and a severe error. We were, unfortunately, magnified by ill-informed people. The process of risk analysis and risk evaluation is and has always been a matter of discussion. Tragedy shaped our view to understand that a risk matrix is nothing other than a prioritisation tool for risk treatment options. Almost every catastrophic event in the mining industry was recorded in one way or another on a risk assessment, yet the very same ones still occur. You can alter the number to suit your perception of residual risk, but the conveyance will still fall down the shaft, leaving its guides or detach, which cannot disappear as long as we use conveyances.

In conclusion, I have yet to encounter any court document requiring the risk level employed to imply stakeholders practised as low as practicable measures. Not once have I seen residual risk used to show that the delict did not take place. As a matter of fact, the event took place, and evidence is required to determine negligence, not whether residual risk levels were met.

Boardroom induced

Risk and Resilience, as a decision, never gets the response the board encourages. Historically, resilience is the ability to return to the status quo after a disturbing event. Many events have shown more harm to a company's reputation than the related cost to recovery. We have learned from the past that reputational harm impacts shares but is short-term in nature. The ability to recover during and after intervention is synonymous with adversity.

Resilience is part of the risk management process and is integrated into the operational demand. Residual risk measures indicate that the affirmative steps alleviate the

risk velocity before and during the event. It is these factors that, when not documented, result in misfortune. The objective must address the root causes, which should have been identified during the risk assessment. Very few methodologies have this subject proactively integrated into their structures; it is mainly a reactive function. A technique such as the Bow Tie Analysis aims to identify these threats, establish control regimes, and show the systems' vulnerability to the board, which will provide resources for strengthening capabilities. We are at a point where boardroom decisions focus on systems perceived as critical to prevent events. Critical control management is overpowering the need for resilience system analysis (RSA).

As shock absorbers, boardroom risk decisions should aim at vulnerability, capabilities, and resources to effectively integrate risk and resilience into strategies and programme planning. This emphasis adds value to programmatic approaches within an articulated, multidimensional, cross-sectoral, and vertically integrated process.

The integrated process requires developing strategies with associated policies and approval by the organisation's risk committee. These policies would have two primary objectives: to prevent accidents and to reduce consequences. Prevention strategies adopted through the risk assessment process are well entrenched in the industry; although companies have a common approach to zero harm, they have significantly different methodologies. Successful managers who have served on various boards would acknowledge the differences. In principle, we have systems that migrate, impacting the organisational risk attitude and industry risk culture. We must note that reducing injury rates is the dominant approach in the boardroom. To show success, fatality rates must decline.

Appreciating the noteworthy effort of the industry to reduce accident rates, companies remain challenged by incompatible risk management programmes. Several have the impartial objective to improve injury rates by alleviating the magnitudes of events; in other words,

nothing different than consequence management, no fatalities but rather injuries. We recognise them in the control regime and legislation as rollover protection, pedestrian detection and warning systems, airbags, vehicle cab design, or automatic fire suppression on a vehicle. A few will advocate tolerance for inattentiveness or recklessness. The last set of control regimes would increase the consequences through irresponsible changes to the work environment, such as narrow roads between structures with a clearance notice, speed humps, spider crossings (multiple roads), crash bumpers, etc. Operators of machinery are defenceless in assuming a safe situation exists when negotiating these controls. Indeed, the control design will significantly increase the outcome if an event occurs because of a slip or a lapse, absentmindedness, or intentional violation. People adapt to the work environment; similarly to controls, they develop a subconscious capacity to challenge controls. Therefore, consequence management is not regarded as a practical approach to reducing injury rates.

Strategically speaking, risk management is about something other than reducing lagging indicator rates. Risk in the boardroom deals with managing the risks to which the company is exposed. These are financial decisions; the above-mentioned is operational risk management to ensure business activities successfully meet objectives. The viability and liquidity of the company is a different approach. Unfortunately, this is where the difference in approach has become an impediment, with little to no movement or success in marrying the two systems. Over the years, the safety risk owners operated within one silo and the financial risk owners in another.

The migration of risk management ideas is inappropriately influenced by demand, in laypeople’s terms, guided by the month's flavour. With the best intentions and founded on sound principles, many risk management programs are launched only to be re-directed by industry incidents requiring priority. In this case, any example will do; a trackless mobile machine runs over a person, and immediate attention is directed to using mobile machines,

their brake systems and interaction with people. We will fail if legislators and managers who do not react well to bad news are allowed to run our risk management programmes. Effective programmes can deal with these events; risk culture should indicate the impact of "the tone at the top"; accidents do not determine the consequences., and the magnitude of the risk source and related velocity.

In conclusion, managers and boardroom risk owners can proactively manage risks. They should be allowed to challenge risk and deal with events if they occur within the parameters of good corporate governance.

Risk in law

The law has an adverse impact on risk management. The matter will investigate aspects of where the law has become too prescriptive, and the fact will expose the legal constraints to risk management decisions.

In physics, the word matter has a different meaning; it takes up space and can be weighed. There is a coincidence because the law takes up space during risk decisions. Time spent on workplace legal obligations can be measured and quantified, thus weighted to a magnitude. If we have a risk source and the law and we can quantify aspects that affect the source, then we have a risk. Companies exist not to abide by the law but to generate income and create wealth and sustainability. Law, on the opposite side of the table, is a highly reactive tool used to deploy how we do business. They were developed because of blood spilt in the workplace, and primarily consequence drives with little insight into business economics. Any economic expert could designate the guiding principles of business economics to prevent your losses.

Our focus would be on the structure and possession of the law to the extent it regulates risk in the workplace. The law and its regulators were the sole owners of the so-called "blame culture". It was apparent in the first section of safety legislation, and still

exists, worded “the employer must”. These obligations are then used to blame the manager after an event, not only by the legislator but also by stakeholders, unions, and employee representatives, and even public opinion has been added lately to the subject. I have lost count of the times the word “the employer must” appears in the legislation. I searched through the Regulations and ended up with over a hundred and forty, still counting as amendments take place. This is compared to only six duties of the employee. No wonder managers are under such immense pressure to comply; it has become a “cult”. It has progressed from a risk culture, making a place for a compliance culture. If anyone is to blame, it should be the legislature.

The fact is that the law cannot manage risk. To latch into the above aspects, the legislature needs to have the capacity or capabilities to govern a mine or any minerals recovery process. They can tighten the nut and limit leverage and ownership of risk. For example, in the 1990s, when the first few mandatory codes of practice were issued, the mining houses complied and submitted their document for approval to the related department. The department at that time had a big rubber stamp on the front page, “approved”. However, after the first fatality, which ended up in a court of law, the manager pointed out that he complied with the “approved” practice. This means that the guideline was very prescriptive towards content and, in its view, regulated by people who should be able to guide in the matter; for that reason, they scrutinised the code of practice and approved the same. The court turned its guns towards the department, and from that day on, it will never again approve any code of practice, exemption, or assessment, admitting the shortcomings. I believe that mandatory codes of practice do not address the realism of risk in the workplace and re-direct onus; they do not provide guidance and are limited in formulating a risk-based approach. More time is spent on aspects the legislator and the drafting team decided to be of

importance. The risk-based approach allows the manager to determine what is essential on their own, not an external drafting team.

The opposite is also true. What was done during the same time frame from a management perspective to enforce a risk-based approach? A mammoth effort was made to search for alternative opportunities to redirect and migrate to a safer operation. In doing so, they established a process that is contained in many best practice guidelines and journals.

Risk in the Rainbow Nation

The influence of historical philosophies on the modern strategic role of risk professionals in the rainbow nation presented a rhetoric risk control framework with lucid principles within the mining industry. Over many years, we have noticed systems evolved and systems that have devolved. This section will pursue the horsepower discharged by key role players, intentionally and consciously, aggravating concepts of risk control in the mining industry.

South Africa is labelled the most progressive country in Africa, though its risk management systems are questionable in many ways. The corporate governance principles displayed by the national and local governments did not uphold best practices and fabricated a risk culture comparable with Gray-listed countries. This culture allows societies and businesses operating within the commerce framework of the mining industry to deploy suitable systems, encouraging the weakest risk management practices noticed in history. It supersedes anything since 1911 when the first mining safety regulations were promulgated.

Compared with the financial sector, which has registered professionals upholding risk governance and compliance, the mining sector produces professional engineers and operational managers without formal risk management education. However, engineers and production managers have established systems that surpass any financial risk control strategy in the mining industry. The difference persists in that the severity is misleading the eye of the

beholder. One cannot hide an accident with injury, and it requires medical intervention and reporting to authorities. Misuse or allocation of funds, petty theft, etc., happens in the background and is only reported when noticed by someone or a system flags the event. Silenced witnesses become risk partners and evolve into a culture of non-conformance; it's the way we do business.

It would not be fair to say that well-educated risk professionals tend to neglect their systems, whereas production personnel managing people's lives pursue best practices on a circadian basis. On the other hand, this just might be true in a rainbow operation.

We have a long way to go with the risk culture in the mining industry. Risk culture is the values, beliefs, knowledge and understanding of risk shared by a group with a common purpose. Strategically, South Africa needs a formal approach to measure any governance or risk compliance culture. In short, we would rather have a culture divided into sectorial zones, with governance somewhat alienated from risk and compliance by role and function. (Winter 2015 RM Professional). In the same article, I have quoted the tendency of having a financially qualified person at the board level responsible for risk. This approach limits the knowledge of material risk control. Holistically, we have deserted the fundamental philosophy of zero harm: saving lives cannot be done by monetary value protection. The doctrines of avoiding loss remain the same for risk, but when maximisation of profits is critical, which is a dialogue norm of board meetings, the window opens.

In the backdrop of the previous statement, let's have a look at a company's annual report. What do you find as measurable and functional governance and risk compliance information? On average, 8% of all critical risk and performance indicators have to do with material risk, and less than 6% have material risk listed as a principal risk. There is overwhelming evidence that protection surpasses prevention. Take care not to misinterpret the latter statement; protection is the practice of managing risk and securing the company's

financial stability, whereas prevention is to uphold systems preventing loss. A project will be terminated, mothballed, or downgraded to protect the company's capex. In contrast, prevention would be deploying a strategy to explore risk opportunities, such as expenditure to install collision avoidance systems with maintenance policies at any cost to save lives.

Who developed this mysterious structure that authenticates complex system drivers and orients managers towards a risk-protective, preventative, or risk-taking approach? Entrenched in the mining industry is the unfortunate influence of catalysts that ascend from the aftermath clouds of serious accidents. The event outcomes and recommendations point in one direction: we have become a protective and preventive industry. Evidence resides in the recommendation versus implementation and legalisation. In other words, recommendations protect the risk owner as the first objective. Implementation is singular at the site where the event occurred, and it disappears within the industry until one day when it surfaces in a legal format. We are sufficiently insensitive to adaptive engineering, and it has become an unfortunate custom to avoid the basic principles of risk management when we do accident investigations. We can conclude that a protective and preventive cult is the culprit in the turmoil of a disaster, in combination with the lack of systems that uphold sound risk management systems. We need to pay more attention to the risk opportunities that may alleviate many of the material risks the industry is muddled with. The industry must make this shift. However, it would be a massive volte-face for the mining and metal industry to change its mindset and adopt a new risk response culture. The principles of risk opportunities and associated response plans will require well-designed policies. Existing systems designed to identify risk sources, assess, and determine residual risk by assigning value from a risk matrix will have to change and adapt this programme addition. Attentive reference is not made to historical treat and tolerate principles; this is an approach where the reasoning of

why we need to track, shadow, and simulate a risk opportunity before anyhow and what outcome is acknowledged.

Embracing a system that advocates risk response activities can be simple. Various systems have been adopted to engage such a process, some too successful and others less effective. A tier approach is such an example, where risks on the lower tier are placed in silos and dealt with by subject matter specialists. The second tier functions independently from the top structure. This detached structure became customary in the risk defence mechanisms for the governance, risk, and compliance framework, which deceptively introduced the devotion to a protective culture. Inevitable and over the years, it has moulded a disjointed process that has caused unprecedented harm to the risk management systems used in the mining industry.

Further misplacement of resources was evident when the industry embarked on an approach parallel to the silo approach, where the physical risk role players were combined into a single function. An example was the amalgamation of the safety, occupational health, and hygiene departments into a single function. The result is that a medical practitioner reports to a risk manager. Legally disillusioned and disjointed individuals were replaced with unconscious, ineffectual observers. For many years, these people were placed on a platform developing and implementing risk management systems for the mining industry. It was only after several disasters that this misstep was recognised, and the role of the strategic risk managers was handed back into the hands of the risk professionals.

Strategies and risk architecture are developed at the company board level, where risk appetite is matured and promoted. The final upper-level risk management framework should include, as a minimum, the risk structures defining roles and responsibilities for internal and external control, the risk management strategy giving direction for philosophies and policies, and lastly, the risk management system having detailed information, audit protocols, rules, and procedures, are approved by the board members. Concurrently, in development, a lower-

level strategic management process would be articulated based on international best practices and guiding principles. Perceptibly, the business risk owner is part of this strategic process. When the strategy is rolled down into the activities function, it shows arrival at the shop floor when recognised by the material risk owner within the verification controls format.

The context of the last few paragraphs affected the Rainbow Nation's approach to risk management over several decades. From good to bad and from bad to worse, the industry has a place for all. I recall a conversation where a risk manager asked me why it is necessary to identify hazards, why we have to establish the magnitude of the risk source, or why we cannot list the events. Another conversation revealed the best practices for critical controls developed to fit a highly demanding and sophisticated plant where QR codes were implemented. There are many examples of irrational applications during the development of the risk management framework. Still, one aspect is clear: future research will show that the mining industry was innovative and made 'ground-breaking' survival decisions during the most challenging times, which include political, fiscal, and legislative changes.

Geotechnical analysis

Risk management and Geotechnical science are synonyms in that both deal with uncertainty and share the objective of minimising deviation from a designed platform of principles. Risk management has a much more qualitative approach and, for that reason, requires support from other similar disciplines to support decisions. One of the habitually underestimated capacities is the value of civil engineering and geotechnical principles that ought to be used during the project and operational phases of the industrial and construction industry.

Let's look at an example of this phenomenon in the typical industrial sector, the road construction industry, compared to the underground rial conveyance industry. Highways built over decades have been upgraded occasionally, in some instances made wider to accommodate more traffic flow, in others resurfacing as repair or for increased load bearing. Slope failure next to these upgrades, roads that flood and water running dangerously on the road during a rain event have become the day's norm. There is nothing to say about gravel road construction; it does not exist. Re-surfacing, on the other hand, brought two weakly thought decisions to the table. One is supposed to be a new and good surface on top of an already disintegrated surface, and the second is the increase in surface elevation. The latter might not be relevant to the topic. Still, from a risk perspective, it will decrease the height clearance under a bridge and result in a truck with liquid petroleum gas colliding with the overhead bridge construction, resulting in a massive explosion with multiple fatalities and injuries.

During the underground tunnelling for rial roads, a mining company would be more sensitive to the behaviour of ground, soil, and nature in reacting to disturbances. Whether that happened because of geotechnical conditions, hydrological conditions or other external

loading forces or stressors, the company is legally obligated to employ geoscience and geotechnical analysis.

We have noticed more than often that the building and construction industry needs to pay more attention to this function. The lack of technical data and the financial gain payoff during planning new housing projects, multiple-story buildings, drainage, and stormwater systems. The civil engineering and geoscience professions meet in different boardrooms. Ask for proof; you might find one or two borehole samples and analyses representing a large-scale project. We can confirm that 2 sample results would not substantiate risk decisions. Although only valid for some projects, it is well-identified in smaller town planning offices. For example, several buildings were constructed on top of a rubbish site, only to show severe structural damage after a few years, which ended in court cases and the demolition of the buildings. Others include where houses in coastal towns have been erected on unstable, underearth material. In conjunction with poor stormwater management, it results in unsolicited ground movement and subsequent structural movement. After investigation, a professional person decided without any geotechnical information.

On the other hand, the mining industry will have a much firmer grip on examining subsurface conditions; the sampling and mapping practices and the analysis and interpretation of information are well embedded in mine design and planning. Geotechnical modelling and rock engineering define the expected behaviour of rock and delineate the response of rock and rock mass subject to the stress fields and the physical environment. The risk of using invalid data leading to a misunderstanding of design problems is assessed using numerical modelling techniques.

The construction and building industry needs to embrace risk management principles. Trapped in legislative directives of having a historical safety and health approach with officer inspections and observation portrays the lagging and reactive approach to the industry. Larger

construction companies have adopted the risk-based approach to their projects and appointed risk professionals with experience to provide the necessary change and systems that support the company's risk appetite. It is the smaller companies that, although law-abiding, need more expertise and capabilities to implement the required risk management methodologies. For them, the reference to risk remains an alleged safety issue; the vocabulary needs to be understood, and risk maturity is demonstrated to be very weak.

Project risk management

This subject is on its own, though the fundamentals and several pitfalls need to be mentioned. Project risk management should be integrated with the company-wide risk structure. If not, separate systems will drive different decision models, departing from the company's objectives.

Project managers exhibit the process; they appoint and guide experts who are conversant with project requirements. One such person should be the risk manager overseeing this function for the project's entire life cycle. This will require a competent risk facilitator acquainted with the narrated risk assessment and decision techniques. In liaison with the project manager, they will assess project risk at each phase and stage and control the “gate” access. It is not the function of the project manager to determine the project risk appetite levels. Based on the risk assessments of each phase, the risk manager should develop a risk appetite statement that imitates the risk-based decisions, diffusing the project capital funding structure. More practically stated, when to pursue risk and when to pull the plug on a project. The latter include when to mothball, terminate, or discard the project or part of the time frames defined.

Lessons learned in project management include the ill flow of information. The outcome is mammoth to project efficiency and key risk indicators. The very same information issue caused a significant number of industry disasters. Construction of tailing

dams with a late delivery date resulted in tailing pumped into rivers for several days. Process plants were mothballed because of capital re-allocation, environmental applications for water use licenses delayed the initiation of a project for six months, and digging up eight-hundred-year-old graves in mid-project phase caused a four-month delay, to name just a few simple mistakes made by a project and risk manager.

All project risks can be classified as either avertible, strategically calculated, or external to the project. Risk response strategies become more challenging when project scope changes aggravate preventable and strategic risks. Take cognisance of the few difficulties associated with project risk management.

Uncertainty: The level of uncertainty varies between Greenfield, Brownfield, and Bluefield projects. Where greenfield projects have limited contains with prior work, the other projects may directly interfere and interact with existing operations with a much more significant impact. It is known that uncertainty within a dynamical system influences risk properties and trends, which produce substantial distortion to risk velocity calculations, deviancies, and sensitivity analysis. Proportionately, diluting data with too much complexity to locate the uncertainty of a future state could delay, derail, or dismantle projects to a standstill. Numerous project monuments are prominently exhibited in the construction industry; they either stand empty and not in use, appear to be a half-built bridge on a new national road or a steel structure rising into thin air. With mining, it might not be that visible, but sinking a shaft a few hundred meters from the design results in production transport costs for the lifetime of the mine.

Scope and context: More involvement from the early stages of the project is needed to improve risk identification. When stakeholder involvement assessments, which clarify the work and social and environmental participation, are neglected, or limited effort is made to

follow a formal approach, the project faces consultation and communication difficulties, transparency is questioned, and a matured risk culture will be obliterated.

Optimism bias: Although optimism is a function that motivates individuals, it may also influence group thinking, and the project team may become overly optimistic about meeting the project objectives, blindfolded to perceive or anticipate the inherent risk of the project. Individuals in authoritative positions may restrain the reality of the circumstances under assessment and the future impact on the project. The cognition of resistance to change is contrary to optimism bias, having the same outcome and being predisposed by a lack of experience in the project domain. Risk managers and facilitators should be able to recognise and list these prejudiced decisions, knowing that they will affect risk response plans.

Reliability of information: Adequate and reliable data are the most critical risk decision factors for project risk management and future operational risk management activities after completion. Monumental disasters often ruined the mining and construction industry, where exploration projects of ore bodies or geological mapping produced less than adequate information to support the modelling process. Examples include the number of closed-off decline shafts in the platinum industry, the difficulties experienced with public train transport tunnelling, and the designed open pit mines that became underground. Undoubtedly, the ultimate mining project would have the capacity to generate its capital. Such a project would include mining the ore body from an outcrop whilst the process plant is in construction. However, suppose the exploration results show significant geological disturbances that require a decline to more stable ground conditions. In that case, the project loses that advantage, which is more severe if an optimistic-biased project or risk manager underestimates this.

Communication: Risk assurance transmits the effectiveness of communicating the correct information, as indicated above. However, transparency and timely communication

with stakeholders have an equal impact on risk response. For that reason, strong communication or the lack of interactional channels can lead to understanding the risk, its controls, the costs of mitigation, and the sequential impact. Misplaced signals effectively influence trust.

Budgeting: It would be inaccurate to refer to project budgeting as an accounting function; from a risk perspective, it is not. Boldly, it is interlinked with the project activities and its time frames, which all come at a cost. It is the single most important risk calculation factor of any project. Extending the delivery date can be detrimental to the success of the project and stakeholder trust. On the opposite side of the coin is the project execution team; if the time frame is to be reduced by not allowing known risk delays, it will have the same stakeholder impact. This equilibrating game is a tangible and authentic risk; project managers need to enable the risk manager to use appropriate risk techniques to identify this risk correctly and, as a team, set the mitigation and response plans in place. From experience, the risk manager is nowhere to be seen during these decisions. The misplacement of risk identification obligations has been shown to curb the ability to observe secondary risks, which cascade down into more minor downstream impacts but, in combination, have a meaningful effect if unaddressed. Questions are later raised about the effectiveness of the risk management system, the ability to manage execution and the risk capacity of contractors. The project risk programme is commonly used for material risk with the primary objective not to cause harm. Are we missing something here? The philosophy of preventing impact includes harm to the company's goals and, for that reason, harm to stakeholder relationships, union trust, employee wellbeing, social environment, etc.

Complex dependencies: Any multidisciplinary, multilateral, and multi-dimensional project can create confusion. The more polygonal and interdependency between functions or project elements, the more the risk of subjectivity or prejudice. Misalignment between

dependencies disturbs defined risk management systems that may propagate outward and upwards to disturb an increasingly more significant portion of the project. The dynamic environment in which projects occur is one such dependency with more uncertainty than any other elements. Influences arise from market trends, technological advances, regulatory changes, or unrevealed events (COVID-19, digging up 900-year-old graves). This dynamic behaviour and the problematic nature of risk make it more challenging to predict any future state or emerging risks and the impact of risk potential.

Companies that foster a culture that values risk management, invest in the expertise and capabilities of risk practitioners and enhance the risk function throughout the project lifecycle provide solutions to the above challenges. Other elucidations embrace an interactive approach, conducting risk tolerance analysis, scenario analysis, research for consequence management and strategic intelligence, and expert involvement with collaborative tools to track risk (forensic scanning and real-time monitoring).

Project risk managers play a fundamental part in the effectiveness of project risk management. They need proficiency and capability to negotiate complexities accompanying risk identification, assessment, mitigation, monitoring, and risk governance within a project. Some key areas of expertise that project risk managers should acquire:

- Understanding of the risk framework associated with the project domain (industry, technology, geography), project lifecycle (cradle to grave), costing (exchange rates to purchasing end-user demand) and resource allocation (internal and external).
- Ability to accomplish operational outcomes by applying diagnostic skills for qualitative and quantitative risk analysis. This should include proficiency in using software tools, simulations, and modelling practices to augment the correctness of the evaluations.

- Unrestrained skills to articulate complex concepts, change (adaptive engineering), and impact consequences (problem-solving) to cross-functional teams and stakeholders by generating a receptive environment to facilitate synergistic solutions.

Frustrating to any risk managers is the topic of human error and behaviour. Fragments of the behaviour philosophies became part of project life. It will reveal itself whenever deviances or incidents are investigated and primarily to support a punitive system deeply entrenched in the project management culture, hence the more significant than average labour turnover with projects. One must understand that human behaviour and its limitations or restraints have an adverse impact on projects; below are a few concepts that should be identified in the early stages of the project and alleviated accordingly.

Managers who demonstrate overconfidence in their abilities and, therefore, intuitively proclaim the ability to underestimate the potential impact of significant project risks. Over the years, managers have developed the ability to seek out specific information that authenticates their existing opinions or expectations. This ability materialises in the boardroom when risk information is purposefully disregarded or modulated. Over time, managers working on similar projects become accustomed to decision-making by dominant stakeholders, even if it does not reflect accurate risk criteria. Combine arrogance, ignorance, silence, and fear of the topic, and a project becomes disaster-prone, a pattern reflected in Groupthink.

Managers who are more risk-averse and unsupported by risk attract production-orientated managers. These managers develop a predisposition to be more perceptive to potential project loss events than to the benefits generated by pursuing opportunities. Risk avoidance decisions are the principal cause of this bias, which impedes the capacity to take calculated risks. Managers make critical decisions based on preliminary information received

that they can reference. Attaching to a subjective fragment of information influences the ability of professional judgment and risk perception away from goodness.

Significant capital investments motivate managers not to abandon ships while still afloat. Escalation of substantial losses and more on the horizon will not inhibit their commitment to the project's success. Retreat or mothballing is not in their vocabulary; they salvage or face the loss. Managers who cultivate a perception during project planning and resource prioritisation that short-term objectives are more appropriate than long-term risks. The phenomenon creates underlying conditions with the potential of attracting legacy risks. The decision underestimates the impact and neglects pre-conditions requiring initial mitigation in the early stages of the project.

To alleviate these human behaviours and challenges, companies should outline an approach recognised for its capability in harmonising attitudes. The approach should comprise three fundamental segments. The first is the project risk management structure, which forms the basis of the management approach. This area sets up structures to manage the project framework, inform the stakeholders, engage different levels of management and stakeholders, and provide assurance and effective reporting systems. Secondly, the risk management strategy sets the methodologies and aligns them with the company's risk appetite. Policies are translated into objectives that will require project result indicators. The third dimension is the project risk management systems, where implementation occurs. The systems provide for designated risk management techniques, protocols, measurements, and verification before reporting occurs.

Enigma of Human Conduct

Honestly and without prejudice, is it justifiable to fault a person for the cause of an accident without stating the obvious? Biblically, humans were the first on earth and the first to change what was already in existence, and he has never stopped since. By pure involvement, we must accept all risks and opportunities created by a person interacting with nature. This same engagement, as old as life on earth, has cultivated the ability to perceive, understand, and judge the ambiguous traits of human conduct. Searching for a timeline that denotes the evolution of human conduct unveiled perplexity and nothing else. The probing through authentic doctrines highlighted one critical aspect: it was apparent that the human mind or the matter, or mind over matter, has confused such a magnitude that we genuinely believe our perceptions and are allowed to be influenced by absurdity.

Research will prove the aforesaid statements with extensive specific reference to the relevant discipline of knowledge. The intent is not to question or repeat any research done over many years by well-known philosophers; instead, it is to create tangible and intangible links to the facts enveloping human conduct and signify its influence on the industry.

Let's start at the beginning: human mind and matter. What is the difference, and how does the one influence the other? I can use an excerpt from The Mind and the Brain, which Alfred Binet narrated. Before we can understand how people associate with conduct, we must extinguish the between mind and matter, the makeup of our being. Mind is authentically the facts dealt with in psychology, whereas matter is the realm of physics. This distinction designates the interaction between the brain (the knowable mind) and the contiguous environment (foreseeable matter). A person acts or reacts to the surroundings within his knowable capacity. How does the said transmit into practical terms related to everyday workplace dangers? We must accept that hazards (danger) have two features: what the mind

must do upon recognition and what the surrounding matter does to the mind through our senses. In combination, we will exhibit our ability to manage the hazard.

Perpetual efforts to manage behaviour and human error persistently endeavour to understand how a person reacts or fails when exposed to danger. Several humanistic approaches focused on the flight and fight part of the human brain and how it functions when exposed to threatening conditions. Anecdotal and qualitative evidence were used to drive the thinking and falsify a perception that it would work for employees under the demanding production stress of the mining industry. This school has gone to the next level by hijacking the perception with neuroscience. Concepts, beliefs, and perceptions have it that the amygdala part of the brain, which acts as a processor of emotions, will release hormones to prepare the body to either fight the source of danger or flee from it. Regrettably, the opposite was overlooked, the state where a person over-reacts or sensibly responds with all capabilities to a threat that does not harm a person. The enactment captures the ability of a person to develop a rational response to danger. Symptoms may include a person who is extremely risk averse during risk assessments with a tendency to underestimate the effectiveness of controls or overestimate the impact of the consequence. For this person, emotions play a critical role during risk assessment discussions and will deliberate or contest unremittingly with a solution to the control framework.

To put all this into perspective, we acknowledge that instinct and emotions motivate our behaviours. In theory, human conduct (behaviour) is an instinct and reaction from the mind upon interacting with the matter, which would be the perceived surrounding danger. The factual dismantling of the thinking process is necessary to understand this reaction or inaction, what it comprises, and where human error mounts. Once uncovered, we could pinpoint human error and how it relates to an unwanted event or energy transfer. Herewith are a few pointers to help you understand the thinking process.

- Actions are the process of doing something, commonly to achieve an objective of the mind. They transmit from a fixed pattern occupied by inborn capacity and repones to a stimulus of senses, otherwise called instinct. The emotions of a person's features allow reasoning from knowable information to segregate right and wrong during the action. What emerges as principal features are negative or positive actions, confidence in using certain sensory perceptions, and intimate survival instinct.
- Conduct is how a person behaves within the restrictions of surroundings, situations, and operating conditions.
- Habits are the repetitive way we do things constantly in the same manner. It evolves from a subconscious state of mind which attempts to maintain an equilibrium between goodness and instinctive ambitions. The dominant disposition encourages the habit of performing an activity in a particular manner. Then, the opposite cannot be neglected, as when the same mindset encourages a constraint against our emotions or a suppression of impulsive actions. The work environment, operating systems and execution procedures provide a breading space for habits. An everyday example of a person driving a dump truck between a loading station on the same road to a tipping point, doing the same thing for eight hours. Note that the reference here is not about fatigue, for which many would immediately point out that there are fatigue breaks and monitoring systems. The objective for the operator is to maintain a certain standard of work at a certain pace, which is the dominant character yielding a habit.

  It is strange how often a problematic event with obscure causes becomes suddenly clear by inquiring into the possibility of habitual contributing factors.

This is so because assertion will seem probable when a witness of the accident describes the task, activity, and method of execution as habitual. The defence to this is that it relies on skill and experience, hence a notion of not being a habit; it is the excellent training and coaching process embedded by the company's risk management system. This would be an incorrect account of the facts, and there is no definite boundary between skill and habit. Righteously, skill is possible only where habit exists, and habit exists where skill has been achieved.

Adaptation during training moulds skills, which pattern habits, with one peculiarity in that habit, make actions easy. A conclusion can be made that work cannot flow without habitual activities. This automation of brain function should be investigated during accident investigations.

- Fault implies a weakness of character that does not meet a desired standard of disposition. A person's mental state plays a significant role in deciding whether the fault is a breach of a rule or a personal action related to a habit. The mental state includes the perception of the person towards risk, the experience, beliefs, and memory of past events. On the other hand, fault can result from an autopilot brain mode or subconscious engagement to another activity, surrounding sound (psychological noise), or reckless omissions.
- During accident investigations, we focus more on the legal fault than the mental fault mentioned above. In other words, negligence, intent, or consent, each having regard to the preconditions towards and trigger event causing an undesired outcome. The investigation process in the industry is well aligned with the process of blaming. Yet, we still embark on investigations that pursue fault only in one direction to show behaviour as intent. Very few, if any, of

these highly claimed methodologies track the habitual or restraining forces involved.

Inherently in error

Enigmatic, we have looked at actions and conduct as two separate functions of a person in the workplace. How does this relate to human error, the ancestor of unsafe acts? In the beginning, before any law, what determined a wrong or a mistake by a person? Who was the superior person who could distinguish between right and wrong? For example, if I am cold, I will seek warmth; when I am hungry, I will seek food. An action for a basic need, how is this different for safety? I seek a daily safe work performance, make no errors, and return scratch-free home daily. Reasoning to content these desiderative actions or conduct whence from effective fulfilment, intellectual or not, will vary in every possible degree.

Unpuzzling the polygonal phenomenon of "human error" denotes several causative features, even though human error remains a thought-provoking and volatile characteristic of humanity in understanding behaviour, actions, faults, and the cognitive process. Note that a few of these aspects will give more clarity.

- Cognition influences decision-making when encountering a dangerous condition, situation, or uncontrolled environment. Realistically, a limitation to bias is diverted with factors such as emotions, instinct, habits, and perceptions. People will act differently when encountering an oncoming vehicle in an underground tunnel. The cognitive emotions will provide immediate action, such as stopping to walk and searching for a safe place to stand or walking by thinking there is enough space between the vehicle and the sidewall.
- Situational awareness and individual differences are characteristics of an unpredictable response. It is challenging to determine in the aftermath of an unwanted event. It varies because of distinct features used to manage stress,

fatigue, or operational conditions. The same person who decided to keep walking with the oncoming traffic works under production stress and has several activities to complete before they can leave the mine. It became the main decision-making feature and made good sense at the time.

- Past, unintended, or unforeseen consequences influence risk perception. The illusion created during the recall of historical events with a significant adverse outcome superseded the lack of information, misinterpretation of existing data sources, or any new-aged simulation. The person in the roadway is familiar with events such as being run over or crushed against an object, yet does not influence their decision. They perceive that they are in control, and the outcome can be predicted.
- The cause of error is sometimes affected by multiple decisions by one person or several people. The ripple effect of the base decision has a downstream outcome that may vary in response. The vehicle operator placed long material on the rear end, which protruded into the area between the vehicle and the sidewall. Another person decided to walk behind the vehicle, as it was safer and in the same direction as travelling. The oncoming pedestrian was blinded by the lights and glare from the vehicle and decided to look downwards to at least note the condition of the footwall, not to trip or slip in front of the vehicle. The vehicle is fitted with a brake system that will automatically start and stop, if necessary, when in proximity to a person. Vehicle drivers and pedestrians became mindful of this system and, over time, were reluctant to accept that it was in a failure mode. The consequence retrains the complexity of the decision to walk or not. However, over time, the safer, new-aged brake

system has superseded a historical decision to stop and await the vehicle to pass.

- Once the event occurs, it is a matter of following a formal, systematic analysis process to determine the human error in the decision. The investigator follows the pre-forma questioning process, which is easily predicted in hindsight. It is worthless to say that the human error thinking process did not form part of the investigation, information, witness questioning or data analysis. By perception, it did because investigators are trained through a one-dimensional days programme. The need for a better understanding of human error and the methodology of determining the information that constitutes the decisions before or during an unwanted event must be included in old and modern causal investigation methodologies. Investigations need more education in any psychological process that constructs human error. Following a questioning line directed by a yes and a no represents an ill system away from goodness.
- As in any risk management system, there must be a form of lessons learned to secure continual improvement initiatives. Identifying opportunities is a function of improvement, not based on human error but on which features of the human mind have contributed to decisions that have ended up in unwanted events. It must take the next maturity step in analysing which decision features constructed the wanted events or have restrained a good decision-making process, delivering good business.

The diagram explains the complexity of human behaviour and the many misconceptions about managing this convolution in the workplace.

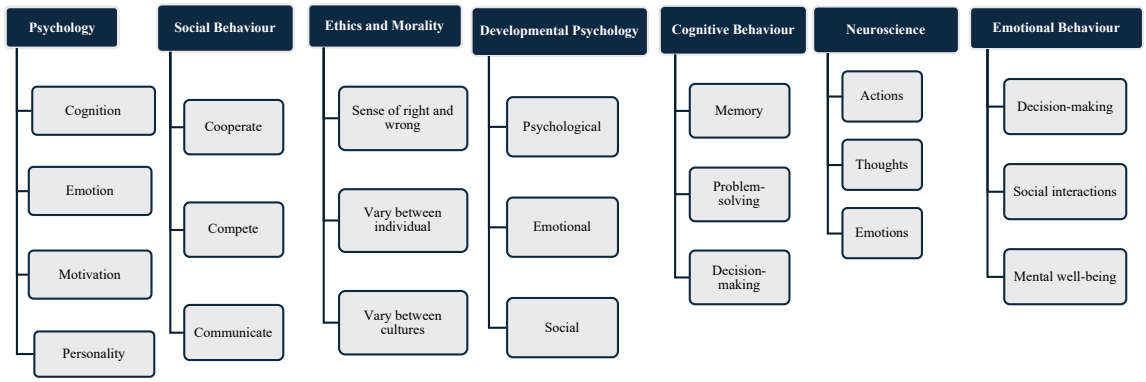

Figure 1: Illustration of Human behaviour

Many efforts exist in managing or improving decision-making with a common understanding; it remains a skill requiring certain traits that will function well with practice. Understanding the human mind's capabilities, limitations, and how it is influenced offers a pathway to understanding behaviour. Risk assessment may neglect this function, but with proper education, a matured risk decision-making model will give rise to a matured awareness highlighting errors.

The industry must direct its efforts from task risk assessment to more potential error analysis. The latter will create the opportunity for line supervisors to close gaps in decision having wanted outcomes. If this cannot be achieved or has limited effect, automation and technology are the foreland in our efforts to zero harm to a person.

A diversion from the so-called near-miss reporting and analysis provides a further opportunity to manage human error. A mature risk management system will emphasise reporting human error and analysing underlying causes. This culture change on the lower echelon of supervisors and employees requires a detailed and definite programme with good communication and trust as intent.

Each person differs in risk perception, how they perceive and understand hazards, the flow of energy, the existing conditions that influence a risk source and many other factors

that give rise to risk or opportunities. The permutation and dynamics between psychological, cognitive, and environmental factors influence this perception. This perception changes over age and the time we spend in the workplace. However, a few individuals need the ability to develop a stronger sense of risk. Reasoning these restraints to act or react to risk has several roots or behaviour traits that become apparent when examining the different stimulus which inflicts upon ability. The following might be contemporary to some, but what we miss during event investigations and causal analysis.

- Settled habits develop while performing actions unconsciously and often compulsively. These habits confirm the dominant personality or character of a person's thoughts and feelings. A formula for these behaviour patterns is exposure to repetition, too long at the same task, or physiological function.
- Persistent behaviour problems reveal disruptive behaviour habits and dissocial disorders. A habit conveyed by rebelliousness, insubordination, the deliberate intrusion of the rights of others, bullying and harassment of others.
- Neurodevelopmental disorders are characterised by substantial restrictions with everyday identification and interaction with intangible risk, societal interactivities communicating risk, and practical abilities to manage risk. It is acknowledged that several other mental disorders also have the same effect on habits, which might include post-traumatic stress, depression, and bipolar disorders.
- Historical exposure branded by beliefs, norms, cultural background, peer influences, social pressure, and some personal traits cultivates different risk tolerance levels. This coincides with understanding potential risk. Lack of exposure to specific risk sources influences the ability to anticipate possible danger in the workplace.

- Cognitive biases and fallacies of individuals settle down into habits that affect either over or under-estimation of risk, or even worse, will stay on the safe side in the middle and never make a decision that will affect their ego. Observed by statements such as “not on my clock, impossible, has never happened”. History has shown that people who deem their ability to estimate and manage risk as always correct, claimed by positive outcomes, become overconfident, which is the birth of disaster.
- Intellectual abilities to understand technical information or cause-and-effect relationships of risk sources. Individuals will develop habits to deal with this limitation and fall back to coping mechanisms such as downplaying or ignoring risk, using generic statements proclaiming understanding or establishing a point of debate in the early stages of the assessment to derail the process and dispose of the function to another department.

It's important to note that risk perception and awareness can evolve and devolve and are subject to the complexity of human behaviour and habits. When a person recognises they have made an error, their instinctual response can vary depending on their disposition, the severity of the consequences, and the circumstances under which they operate. Denial, increased work stress, guilt following a fatality, apology, seeking assistance, and blame shifting are but a few factors that can easily be identified in the aftermath.

The diagram summarises the state of intricacy of human error in relation to human behaviour from the previous diagram.

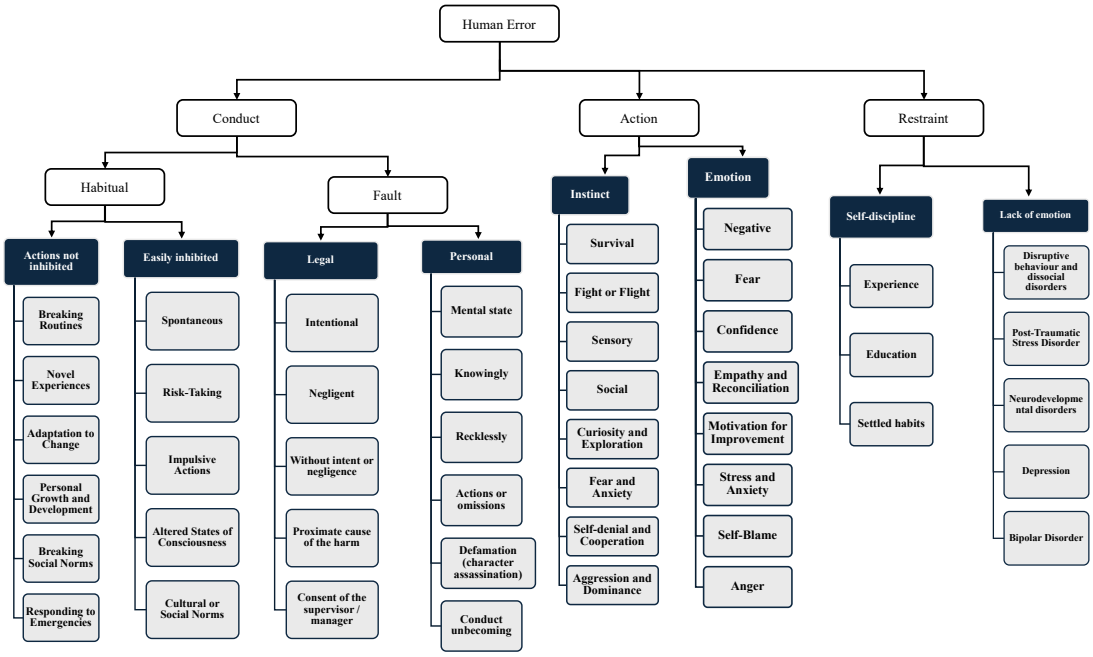

Figure 2: Human Error

Psychology behind Casino Safety

It is an exciting subject that, under most circumstances, is avoided in risk management for unsubstantiated reasons. Many risk consultants and managers circumvent the topic because of an absence of understanding of the indebted wisdom owned by the philosophers. Risk uncertainty has forever exposed a few psychological concerns in the workplace. References to previous topics touched on a few subjects in this field, but the consciousness behind how we perceive risk remains debated. Nonpareil to discussion in a casino, virtually resembling “casino safety”. A fool is as good as a gambler; they think they are wise and believe their prejudice is correct, so they keep being stupid. Stupidity is the opposite of intelligence, corresponding with day and night. There are conditions where the day and the night meet, either dusk or dawn. Thou far apart, it gives rise to an intermingling period, a short phase where stupidity meets with the intellectual. Otherwise stated, where

intellectual people make reckless decisions. Carelessness at the base of recklessness is directly connected to the likelihood of risk; influencing figures of a risk matrix by perception is no different from gambling. It converts into a habit and formulates group thinking in a boardroom.

When the topic surfaces during a risk assessment, people tend to fall back to their intellectual capacity and related habits; if it becomes too technical, they use a generic attitude or methodology. It is no different from gambling; the event is subject to the fall of the dice. During the facilitation of a risk assessment, people may encounter technical difficulties in understanding a specific risk source and how it may change or drift into a new phase and transfer to an alternative control framework. As an example, the pre-conditions for the failure of a hoist rope. The Engineer will meditate that it has a safety factor and remain conditionally safe until that limit has been reached. The risk assessor starts at zero distortion of the rope, and any deviation increases the likelihood of failure. The person without knowledge of hoist ropes will argue that the rope will fail, no matter what actions or factors you work with; the gambler is interested in the outcome, not the likelihood.

Horizon scanning for any risk assessor is a nightmare, especially if you must find a middle way between recklessness and proper risk-taking principles. Unfortunately, the mentioned gambler refuses to let go; from his point of view, he judges everything against his view, a good indication of the origin of absurdity. Such a person will remain quiet during the identification process. Still, when it comes to risk levels, he will argue meaningless issues for hours to derive at the same point where all of it started, allowing him to find his way to believe it was his decision. This egoistic one-eye syndrome has decorated many disasters with blood. Phycological constraints embedded in person may be the single most significant mismatch of risk management systems. To be wise is as dangerous as to be foolish. Objectivity is what the wise man would suggest, and subjectivity is for the fool.

Let's take a walk down memory lane and individualise the behaviours, conducts and habits of the wise and imprudent people. A legal obligation is to ensure people are not exposed to thermal stress that may cause any illness related to high or low-temperature levels. Wisely, we would include as many factors as possible to assess each person's risk profile, which would be under our control. Recklessly, we would generalise and adopt a temperature level where the exposure will harm an average or reasonable person, the most common dominator as a benchmark. Any person not above the dominator level is at a higher risk than one above the dominator. A person collapses during the re-entry of an underground workplace. During the investigation, the focus will be on the obligation status. How does it happen that a person was exposed? Whether the risk was low or high in rating, if the wise man or the fool determined it, it does not matter. The question comes from the investigator's intellect. Legal obligations have one thing in common: in any event, someone must be in breach, and the only outcome is to blame someone, which is what the investigator will find. A low blow to the practice of proper investigations. The mere fact that a fool oversees an inquiry that, in the end, may put a gambler in jail. It cannot be acceptable in an industry where so many persons are exposed and the seriousness of our efforts to avoid major events.

Other critical psychological personas influencing behaviour and habits include imitation, passion, affection, and emotions. The most common is the disposition of imitation, which is significantly common where the leadership style or risk culture allows this instinct to propagate. Although a fundamental trait of intellect will contaminate the culture of risk-taking to the extent that a norm is created, an uninformed persona may contemplate the temperament of a leader. Mirroring a predecessor is as foolish as industrial suicide. In its worst form, you may find a front-line supervisor who has the same habits as the section manager and, in turn, emulates the general manager.

In criminal psychology, passion and affection are said to be a feature of an individual mind. It is a subject of confusion and influence, affecting physical emotions. If the passion in which a person performs a physical activity appears devious, we label it as criminal; if it is the opposite, we tend to influence the perception of character. The desire to reach a defined outcome during the execution of the task has the purpose of care. Both desire and care affect emotion, a leading characteristic of observation, and what you see is what you get. Certain individuals will show fear of risk, and others will not. They are not criminals because they have little or no fear but tend to challenge risk with a similar mindset. The prosecution of a criminal has not stopped similar criminal activities. For example, the successful prosecution of a white-collar crime, such as fraudulently transferring company funds to your account, has not stopped the crime. There has been an increase in this form of crime, even with jail sentences of more than 30 years.

Similarly, risk-taking has not been reduced in the workplace because of the successful investigations, the blaming of individuals and attempts to change behaviour; it has somewhat increased, just in another form. Think about it: How many accidents on the road occur because of emotions without being subject to road rage? Still, the inactions of other drivers heavily influence the desire to get safe to the endpoint. Correspondingly, in the workplace, fellow employees and your surroundings provoke your emotions during the shift. Prolonged exposure to these emotions transforms into habitual responses.

The paradox of psychology or the safety mindset is furthered by several mistakes, which include our senses. The mind uses the senses to detect our surroundings. Hearing, smell, touch, sight, or taste detect physical risks. For the intangible risks, we must use senses such as cognition, behaviour, or perception, as referred to in our gut feeling. These sensors connect our instinctive actions of flight, fear, or aggression. Parental emotions are emotions that either draw people together or push them apart. Unfortunately, everyone has a different

sensitivity to each of the senses, affecting their judgement of risk and subsequent conflicting behaviour patterns. Arrays of mistakes most known in a work environment are distance, illusions, and reflection.

The judgement of distance has been a topic of discussion for many years, and it is not the professional golfer who is good at distance judgement; it is the caddy. A workplace distance from a risk situation may mean the difference between life and death. Such as the distance of the outflow from a tailing dam, the local community may perceive it less and build houses closer to the risk area that the operator of the tailing perceives. Optical illusions may also influence distance judgment. In underground workings with limited illumination from the light beam of the cap, the lamp may create tunnel vision, ideally for optical illusions of surroundings. The latter remains in the mind and is recalled during investigations, leaving us with misleading interpretations of pre-conditions, event sequence and causes. Considering that the light beam has also limited the eye's ability to judge an object’s size, it highlights the vulnerability of the correctness of information during pre-task risk assessments or later provided by a witness. When the situation is intensified by virtual simulation, we are thunderstruck by how fundamentally fabricated our perception was, abducted to culpabilities of memory.

Risk assessors and accident investigators should be aware of the magnitude of these deviations. The possibility of error in distance and size judgement according to reasonable standards is undoubtedly inadequate at undefined magnitude. Psychologically, it appears to become a habit to accept the illusion of distance and size; we do not pay any attention to it and instead generalise.

How do we deal with the enigma of behaviour, and where do we focus or what is next? Will a psychological approach solve the problem? In essence, no, there is no quick fix, a book from any shelf, a short classroom educational programme, or a behavioural-based

system. For many years, the industry indulged in similar programmes. Sometimes, they are still approachable and misled by people with a distinct sales pitch. In my professional opinion, the biggest money-making hoax of the last two decades has shown limited to zero results. The only solution, not based on opinion or perception, is to:

- Cultivate powerful habits.
- Generate detailed industry-specific laws, regulations, and compulsory rules.
- Furthermore, alter the risk assessment capabilities to identify the inciting causes within the human capital or intellectual properties of the operation or industry.

It appears to be evident that the latter can never happen because of the lack of understanding of the risk source we try to manage. Too many people pull aggressively in opposite directions, too many nervous systems generate alternative emotions, and too many act foolishly. Everyone is for himself, and no one is for a person's brain function. Health and safety personnel, risk managers and supervisors cannot be psychologists. Still, we must understand the risks of human actions, habits and actions when performing our duty to care. Incidents are inevitable, a fatality, an amputation or a near miss. Where there are people, there is a risk event. Worldwide attempts were made to stop accidents in the workplace. Using a conference podium, journals, political platform, or judicial finding will not provide for the cessation of risk events. People who still believe they can stop the advent of risk by controlling their human instincts have detached from the profession. Any person who thinks they can influence human conduct permanently and prevent accidents must understand the human brain's fundamental nature, its purpose and what inverted power it comprises.

Forensic Investigations

Understanding the investigative objects in the mining environment has been as troublesome as the risk assessment process. Confusion, misunderstanding and blame-fixing are so entrenched in the polities of the rainbow nation. Over the years, layperson omissions have created scenarios where even the professional believes the ailing investigations are reasonable. Very few, if any, observe the methodologies in use were designed by persons without adequate legal qualifications and background. Take, for example, the technique of incident causal analysis model developed in Australia by a person who worked as an engineer in the aviation industry and later at a mining company, which saw an opportunity to establish an internationally recognised investigation tool. If I understand correctly, an engineer rewrote books on a subject as old as civilisation, starting from the twelve tables through the Roman Law written by professional jurists until today. The methodology was based on an error model created by a professor of psychology. By now, you should know my reference is to a method such as ICAM, of which none has any reference to professional investigative methodologies except fault finding by a person. The theme of following a specific sequence of questioning, like "Why", creates non-factual outcomes; people are not challenged, and they are allowed to fabricate incorrect details truthfully.

Moreover, the analysis prepared on ill-investigated events produces ill comparisons that create the illusion of correctness. Investigating the consequence of poorly designed accident investigation methodologies took work; it simply boiled down to poorly trained, non-professional people who use a window to peep into inaccurate information and make comparisons to create the impression of being correct. As mentioned earlier, the false sense of correctness has become a norm in the industry and is acceptable to the professional. The overseeing government body has no legal obligation other than to investigate, with or without legal background or experience of law. Their findings may finger-point persons for

prosecution, and the validity of the comparison between mine regulation, perception of the breach, and the law makes us find ourselves in abortive.

Avoiding the detail in determining the factual causation in law and using the “but-for” test will prevent the industry from developing effective remediation. I believe that the time, resources, and effort wasted on poor investigation demonstrate the number of work stoppages issued by the inspectors and the holders of the system. Very few have the knowledge to show effective investigation; no person or institution verifies the correctness or quality of any investigation, yet we use causal analysis for predictive monitoring. These outcomes end up in legislation similar to the pedestrian detective systems on vehicles, which create an illusion of perception that it is the correct thing to do. Without accurate investigation data and understanding of the data modelling process, any conclusion is likely flawed and can potentially deceive the industry. Our old-fashioned methods draw only raw data, nothing different from information. What is required is the definition of the intelligence of the data and work done on the data to give added value or significance in the context of the event. I do not conceal for myself the arbitrary of my own opinion, but this is something we cannot avoid. The ineffective and ineffaceable contras of knowledge offer disasters yet to come.

A successful investigation does not have legal liability or prosecution; it meets the principle of legal causation of an ethical quality. Investigators and the legislator must stop being naive and recognise a process's capabilities based on sound legal principles. They are not compelled to determine the position of the injured concerning the person in charge; they do not have to find a law somewhere in translation which was breached or question the action to become an infraction through the misplaced forces of logic. It would be fatal to reflect on the decreasing trend in the industry. Disasters still happen, conveyances falling down shafts, flow out from tailing dams affect communities, and labour disturbances cause havoc at the

entrance. The old school has been assigned success in lowering the frequency of major events, but the new school will have to decrease the consequences.

Forensic investigations are widely used, and the literature is comparatively rich, founded, and fundamental to the industry's needs. Formerly, the classical human error school stood alone with its varying shades of opinion of what is effective and valuable investigations, which method is more appropriate and who is more correct in the outcome of the priori of human error. The body of forensic principles is overwhelming in the diminution of events and consequences, and more so regarding the theory.

The industry must define and regulate where to go from here on. The best practice would be a critical look into what is happening with other comparable systems. Better systems may be more time-consuming, as for accident prevention, they need more accurate and reliable data, a solid foundation, and access to comprehensive research. Forensic proceedings have several compulsory critical elements. The integrity of such a system is essential to show due care, diligence, and consistency of information.

- Trained, experienced professionals conduct investigations. To gather correct data and information, one must understand the risk sources, release mechanisms, and related causes. This will require a person who understands research methodologies, has the capacity to draw conclusions, follow lines of defence, avoid assumptions, and draft formative remedial recommendations. Maintaining the integrity and trust of stakeholders necessitated a person who had exposure to a judiciary function.
- Involve a wide range of disciplines. Contributions from experts and scientists are pulled into the investigation at the early stages. In some countries, investigations of major events are done by universities with the capacity for

knowledge and research in all disciplines. This approach also secures impartiality and standardises the methodology.

- Follow the line of information proven to be factual. Access to forensic engineering, forensic psychology, and digital forensics are but a few aspects not imminent in today's accident investigation. A quality investigation follows a process that validates information and evidence before being classified as factual. It may entail back analysis by professionals, ensuring accurate, reliable results.
- Transparency in documentation supersedes all those mentioned earlier. An investigation that is questionable in a court of law or cannot be understood by the general public or witnesses is bound to fail. The credibility of the investigation depends on the transparency upheld during the in-loco investigation, classification of evidence, evaluation and analysis, interpretation of evidence, and fairness of the outcome.

Employing any format of forensic investigation will require a total revamp of the regulatory and operational approach. It may require distancing us from the current legal obligation and having independent investigators walking around the premises. We will have to allow them to take photographs, take biological samples, take custody of documentation or data, and interfere with operational activities. It will require an already mature company that aims to shift to a top level of maturity and that has distinguished the prominent range of influence deriving from a forensic investigation process. This challenge has been at the industry's door for the past decade, and one can only decide who will open the door. Forensic investigations will play a crucial role in our pursuit of safe operations.

Hypothetical unpremeditated

Many risk assessments have used risk event descriptions related to inadvertency, such as the inadvertent movement of a dump truck. Theoretically, a correct description, however, to pin an event to the unintentional is equal to carelessness with a causeless outcome. Bow tie analysis is a risk assessment technique widely used in the industry; it uses an initiating event and determines the causes and consequences of these events. It is here where uninformed people take significant retreating steps. Ignorant facilitators decided that almost all events are triggered by an energy's unintentional or unplanned release. Perhaps the reasoning is that nobody plans to cause an accident, and only criminal crimes happen with premeditated action. However, existing investigation techniques follow a pathway of finding deliberate action or omission of a person responsible for the harm. How wretched is a system that, on the one side, focuses on the identification of unplanned events, but when it happens, the very same focus changes to find intent; otherwise, we protect ourselves with slips, lapses, mistakes, and exceptional violations.

Two dump truck drivers reversed out of a congested parking lot after a thorough pre-use inspection, a safety talk, and an awareness discussion, causing a minor collision. This happened with vehicle collision avoidance retarders installed but de-activated in a congested parking lot. Hypothetically speaking, the event happened unintentionally; neither of the drivers planned the collision.

A laboratory assistant accidentally bumps against the outlet valve of a chemical container whilst setting up a product cleaning process, leading to a small spill. Because the chemical was hydrofluoric acid, and several persons were exposed, it became negligence on behalf of the assistant.

These examples are just a few out of hundreds that signify manipulation when inappropriate investigation methodologies are used to characterise the artworks of everyday inadvertent or unintended events in the industry.

Factually appropriate

Extending the discussion is the historical human error analysis. In the past, most accident investigations had a broader framework for human factors in relation to task execution. Factual investigations disregard the use of assumptions that people will, at some point, make a mistake during the execution of a task. More appropriate systems will have an integrated approach examining a broader spectrum of analysis beyond artificial simulation. Altering emphasis from reactive to proactive requires investigations on risk source events during the risk assessment process, without witnesses, where external influences are dissolved with reality checks on control effectiveness, and where resilient systems show opportunities.

In layperson's terms, criminal law is based on previous events, factually correct, premeditated, or not; if causation is proven and a few other facts, the guilty are charged. The industry already has a drive to develop similar control frameworks to prevent significant events, displayed in drafting critical control standards. Take one step back; the risk sources are the same, the trigger events the same, the outcome the same, and the causes the same. Why is it necessary to spend so much time on investigations if the proactive risk assessment can do the same? Why do we have five days for investigation and only a few hours for risk assessment? Silent witnesses from history cannot speak, but those close to them can reveal very little was done before. From experience, the average time spent during a risk assessment on a single hazard or risk source is approximately fifteen to twenty minutes, including the recommendations and capturing of the information. If we change this approach, we will remain factually correct regarding the outcome of the investigations. The legislature requires

investigation; they get involved, recommend actions, and have the right to issue fines. However, they are absent during risk assessments.

Accident investigations are complex processes that require meaningful input from all stakeholders. Realistically, accidents should not be investigated but analysed in the context of the appropriate risk assessment. This will highlight mature organisations of the future where trust prevails.

Causation path of a system failure

Event causation has been a topic for many years, and the objective is to unpack the correct sequence of occurrences leading up to the event. This is typically referred to as the causation path. Although system failure is a confirmation of opportunity, they never go through the same failure analysis and only consider them as causes. Accident methodologies discontinue when underlying causes have been identified. Understanding the causation path of a system failure is crucial for response and prevention strategies. The reliability of systems has several aspects in common that will uphold their effectiveness.

- The context and scope of the systems are defined in measurable detail to allow for a monitoring regime. Any system without key system monitoring indicators has the potential to fail under certain demanding circumstances. These monitoring indicators should at least include the number of times the system has been challenged and the number of times it has indicated partial or total failure. Having a fitness-to-work examination and evaluation of employees for job placement is only effective on the placement date. The dump truck driver develops a heart condition and fails to report the condition because of the risk of losing income, which is but one example of system failure. The minimum age for operating mobile equipment on a mine by the same code of practice is twenty-one. However, drivers with a code eight

license are allowed to operate under another code of practice, a total disconnect between the two owners of the codes.

- Trigger events are the same as those identified in the risk assessment, so why they must differ during an investigation goes beyond mind. These events should not be the same as immediate or underlying causes, and the reference would be inappropriate and away from goodness. Trigger events have pre-conditions, and pre-conditions have causation within a system. It will reveal the operational environment in which the systems were developed and how it adapts during change. A person's state of mind will disclose the system's breaching capacity, how it will be challenged, and the reasoning behind active failure pathways.
- Contributing factors are factual influences and should not be mixed with uncertainties or assumptions. Any uncertainty or assumption, although documented, should be disregarded. In most investigation analyses, human factors are classified as unknown or subject to an assumption of the investigator or witness who has little knowledge of psychology and how to determine the state of mind before a trigger event. Any review of investigation outcomes will show human error was identified and used as a fact to pinpoint fault, action, or inaction. A grave weakness of the existing incident causal analysis methods and the why-questioning practices used in the industry facilitates the opportunity for improvement.
- Reliability analysis holds the function of detailed monitoring and evaluation of equipment. The same principles should be applied to system reliability analysis. The methodology used to determine at what conditional state a bearing or shaft of a motor would fail can be used to determine the threshold

of a system before a failure will occur, in other words, the capacity to withstand interference from a person or environment. The primary transformation is to superimpose the quantitative reliability engineering methodology to a system reliability methodology currently subject to qualitative decisions. A distinctive system reliability analysis requires a simi-quantitative technique that enhances and validates decisions before the change recommendation.

- Traditionally, organisational factors include, apart from others, the evaluation of the context, policies, procedures, training, and culture. Renewed event analysis has organisational factors as the focus of the tone at the top, management involvement, and the design of the risk management system. Event investigation forms an integral part of the continuous improvement modelling. Simulations of events and their impact on reputation, the social impact of the operational environment, and governance are important.
- Continuous improvement is defined as the objective of improving systems. After a desktop browses through existing investigations, a summary of findings shows that a distinctive process is followed to find fault, identify root causes, define opportunities to remediate fault and learn lessons. A slight misstep made at the beginning of the investigation to follow a pre-defined questioning pathway was a huge oversight. The improvement of systems inhabits capacity, and if capability analysis lacks the ability to identify a system's actual effectiveness, efficacy, and efficiency, it is flawed in design. Drafting a procedure, reviewing existing risk assessments, enhancing training, disciplinary action, and changing the design of a take-up pulley on a conveyor

all have one thing in common: they are not system improvements and will not ensure continuous improvement.

The methodologies deeply entrenched in the industry, which have so many devotees, have revealed their own colours, have been exposed to be incomplete and entertain a need for change by professional people specialising in forensic investigators.

Ambiguous Control Anomalies

The international guidelines define control as anything that modifies risk but might not always employ the intended outcome. The definition devotes ambiguity to interpretation, perhaps the reason why risk facilitators and managers put anything at the table without understanding the objective of control. On the other hand, anomalies suggest the unexpected, whether a deviation or irregularity. The variance in perception gives rise to uncertainty, and uncertainty is associated with an event. In summary, ambiguous controls, which imply a lack of clarity and difficulty to understand, hold employees and systems at ransom; it has an element of expectancy of malfunctioning and undermines continuous improvement.

Material risks in the workplace have event controls primarily designed as a legal requirement and, for that, have the limitation of undisclosed opportunities. People naturally tend to do only what is expected; anything more might expose a manager legally. The more can be defined as a control that has the potential to fail. Thus, we would instead use a generic approach, back to the gambler issue. Whereas intangible risks, such as cyber-attacks on payroll, the controls appear to be obscure. There may be a good cybersecurity reason behind not sharing the control intent or actual context of mitigation. The same is true of security intelligence risks in the diamond industry. Similarly, with complex systems where the dynamics impede the identification of system behaviours, it is challenging to implement system effectiveness monitoring regimes.

Matured risk management structures can define these areas where ambiguous control anomalies appear within a system. The process capitalises on a detailed analysis involving intended system behaviour, anticipated deviations, and effective response plans based on risk velocity and critical control points in a quantitative format. It often includes periodic system diagnostics followed by detailed system forensic investigations which unplug vulnerabilities.

The regulator typically defines risk control measures following significant events in the industry. Very few of the disaster was not followed by a change in legislation. Unfortunately, many of these instances resulted in the devolvement of the control framework. For example, a conveyance plunged down a shaft for various reasons of failure. In the form of a directive, the legislation issued instructions that whenever a conveyance transports people, there will always be a winding engine drive at the footplate. The industry has several winders that operate automatically. They were installed many years ago and operated successfully, and they were never subject to human error in the operation; that was what automation was supposed to do. It was always regarded to be a safer option. The instructions have pushed the industry incorrectly by placing the human error factors back in the firing line. It should be acknowledged that qualified winder electricians and technicians drive these automated winders manually under certain conditions. The existing winding engine driver does not have the knowledge or experience to do the same function. The legislature has not only overstepped its rights, but it also needs to involve professional engineers familiar with the automation and design of winders and provide proper instruction to the industry.

The concept of risk control

To appreciate the concept of risk control and risk response, one must revisit the historical categorisation processes and compare them with mature contemporary strategies. Primordial and slightly not-so-old fundamental concepts include the hierarchy of controls, the Swiss cheese model, trigger actions response, barrier analysis, control matrix products, layers of protection, control failure probability, control reliability, risk responsiveness, and many more. Each has a specific purpose and individually contributes to the countless delusions of effectiveness of risk control. Risk architects thrive on these systems, creating a theatre filled with scholars ready to change the risk world. Changes have been made to these theories, some with good intent and some to disaster. One such example shows the addition of an extra

layer of human error to the Swiss Cheese model by James Reason. These practices intersect with carelessness and create confusion.

Sadly, the same architects produced systems of exclusion to the use of control effectiveness. There focus changed to manipulation of concepts of risk outcomes, by doing this control effectiveness cannot be measures. Once a control has been established, they will fail the control and use that failure as a hazard or risk source. For example, roof bolts control the convergence of an underground tunnel. Inadequate installation has the risk of falling to the ground, so inadequate support for them will be the hazard or risk source, neglecting the fact that the latter has stayed the same.

Additionally, they will reason that the significance of an event is a combination of the likelihood and its consequence. The deliberate diversion from the objective allows a downplay of the actual risk level. For example, a risk assessment identifies an event of a collision between a bus carrying more than fifty employees to work and a third-party vehicle. The architects spend ceaseless time on the likelihood of all passengers fatally injured. The actual discussion was a simple and easy decision: What is the likelihood of the event, and only after that is the maximum reasonable consequence, considering the number of employees and passengers of the second and third vehicles involved? The risk ranking has become so crucial in our endeavour to show management effectiveness in controlling an event that we dilute the risk management objectives. The process has devolved further, and we now have inspectors who insist on a second risk ranking process to ‘show improvement impact’ of controls.

The black swan metaphor described by Nassim Nicholas Taleb gives insight into significant mining events we have underestimated for many years and how we react unpredictably when they occur. The current risk matrices used in the industry have overcome the principles of combining likelihood and consequence; the consequence ranking will

always prevail. Only as long as the definition of significant hazards focuses on the consequence, with the total casualness of the likelihood.

During a mining conference in 2011, I delivered a paper on the black swan metaphor within the context of the mining industry. During research and discussion, it became evident that the industry is busy with activities, which is believed to decrease the number of fatal accidents.

Confusion is a matter of misconstruction of principles and numbers per se. For example, a room filled with risk experts still to be convinced that a consequence signified by a number from a very subjective impact classification will change focus, change a decision to reallocate resources, or serve as a measure of control effectiveness. Should a lower number at least show better control, or should it not? Discuss the factors of human behaviour or human error, and the behaviourist, who is unsurprisingly convinced of managing risk through neuroscience principles, stands back for the scandalous confusion. The number game is more readily accepted when the point of prevention control is misplaced at the unwanted event while it should be at the trigger or initiating event. These scenarios occur daily when a risk assessment deviates from the primary and essential practices.

Fundamentally, control philosophies should entail two essential features that give rise to risk. In other words, the calculated predictions that a specific risk event subsists and the consequence or impact should such an event materialise. Each can be subdivided into many more features, including risk velocity, risk magnitude, hazard drift, and risk deflection, which all form part of the control framework. The low number in likelihood or probability does not mimic a risk event that will not happen soon, and it may happen any second after the opinionated risk assessment. Analogously, decisions were made in the boardroom before the Challenger disaster: ‘If you do not have quantifiable data to prove that the O-ring will fail under these conditions, then I suggest the launch’. It is not the intent to question the

complexity of these decision-making processes. The objective is to question our ability to define control effectiveness and our capacity to manage a quantitative monitoring system.

The control heuristic discloses myths enclosed within the hierarchy of control. The industry uses risk sources to do business; they have electrical-driven hoist motors, which cannot be eliminated. Eliminating risk in the sector is a fallacy; it will not happen in our time unless the interpretation is that replacing coal-generated power with solar power represents elimination, or removing an electrical cord on the floor prevents a trip and fall event and, therefore, simulates elimination. This old-age way of thinking proves the low maturity of people who assess and manage risk. Matured managers understand that we identify risk sources and adjust them to a state where they offer a resource and where we have the competence to manage any outcome or change.

Administrative controls depend on a person's actions, the interaction's behaviour, and the implementation's practicality. People do not act upon risk based on what they are exposed to during a task but on what they perceive the risk to be. They assess risk by emotion, where the control heuristic meets the decision. People tend to feel they control risk the way it was done in the past, and although they have yet to formalise, it is sufficient for them to reach short-term goals. Administrative controls are, therefore, easy to manipulate or change to suit personal disposition and get the job done.

Personal protective clothing is less effective than administrative controls. It is somewhat skewed and misplaced. Take, for example, the full-body flash suit of an electrician doing fault finding on equipment. It must be done in live mode; administrative procedures for performing the task must maintain the effectiveness of the flash suit. The same is true for a symbolic sign to wear goggles, which is perceived as administrative; the goggles themselves cannot supersede the sign.

The subject's realism is that a control has an objective, and the aim should be to captivate all the risk modifiers. The latter are divided into two distinctive mechanisms: those that release the risk source and those that manage the event.

- Essentially, the first and best option is to set objectives so that a control prevents or mitigates the modifiers and not the event.
- Measuring the effectiveness of controls will correspondingly be divided into the same two sections.
- The main interest is the first objective, where prevention and the likelihood of the event are managed.
- The second objective, where we set up controls for mitigation, is a subject of consequence management and alienates us from the ‘no harm’ philosophy.

The paradox of adapting from the old-aged to the new-aged approach to risk is incredibly slow in relation to the fast-growing number of control demands for developing technology in the work environment. This lagging effect has the potential to impact the understanding of control effectiveness, whereas absolute monitoring systems remain in use for newly developed, complex, and sophisticated methodologies.

Control effectiveness

The definition of effectiveness is the degree to which a control can be confirmed to be successful in producing the anticipated objective. In other words, the effectiveness of a specific risk control provides information on how often the associated hazard release or trigger event was encountered and what the control's tangible performance was in accordance with the objectives.

Control effectiveness reflects not just the ability of controls to manage a risk theoretically but also their actual effectiveness in terms of:

- Consistency.

- Reliability.
- Survivability.
- Compatibility.
- Timely operation on demand.

Effectiveness ought to be expressed in quantitative or qualitative terms and can be either absolute or relative. It is usually reported together with a measure of residual risk.

Control responses are measured as the ratio between the times a risk control was challenged and the number of times the control successfully achieves the intent. It assumes an operational key risk response indicator if the response is observable, specifiable, and quantifiable. Many of these matrices have been developed over the years with credit to the originators who paved the way for understanding an effectiveness measure's expectancy. In essence, it includes items of the number of challenges versus failures over time. Herewith a few examples in order of priority to explain such a measure and the variables to consider:

- A mobile machine's pedestrian detection and warning system was designed to identify a pedestrian at a specified distance, send a warning signal to the operator and the pedestrian that they are in proximity and require action, if necessary, to start and stop the machine automatically. The most obvious measure would be the real-time data from the electronic system that indicates the number of interactions versus the specific responses taken.
- Alternatively, during planned maintenance, tests are done on the operability of the electronic system. The intent is to develop usable data for the number of times the control was tested, the number of times the control has worked to design, or the number of times the control fails during a test.
- Post-event measures can also be used, such as the number of unwanted events recorded after the new pedestrian detection control was implemented versus

the number of events before the control was implemented over a specified time frame.

- The same electronic system has a built-in function to override the detection for specified scenarios, such as inside a hard park bay, a workshop, or a congested area at the loading pad in an open pit where the machine parks next to an excavator or shovel. The bypassing of the control renders event opportunity, which should also be measured. Thus, the number of times the pedestrian system was bypassed and the number of proximity detections recorded. Note that the system will still record the encounters but will not activate the design response under these circumstances.

For all control effectiveness measures, an unambiguous description of the control and its intent, the hazards and trigger events, the design qualification, and the operational performance levels is necessary. It is also essential to define what constitutes an unwanted, intermittent and wanted failure of risk control.

- Unwanted failures would constitute a flow of energy in an unwanted direction, a release of energy towards a target with a negative outcome, or a loss of the structure's integrity. These failures only have a negative impact on objectives, can be identified in the early stages of the failure event, and can quantitively determine at what point failure is imminent. If the risk assessment has identified the correct point of failure, it would be a matter of conducting a back analysis to determine the critical point where the situation can return to normal. This is where the correct objective of the control should focus upon, and effective response can be measured. The engineering function led to implementing equipment and structural condition monitoring systems. Unfortunately, there is a clear indication that the system has deteriorated to

reckless levels for many reasons. The financial decisions, cost-lowering practices, and purchasing objectives have altered the best and worst practices, from preventive maintenance to breakdown maintenance.

- Intermittent failures represent the ill-designed systems where periodic failures occur, are not easily defined, and are without notice or indication. These failures show cracks in existing controls. On the contrary, less intermittent failure is interpreted as a control that performs its designed function to a certain extent and, therefore, at an acceptable level. Any control reliability evaluation system that uses a qualitative monitoring process based on a percentage of acceptance levels inevitably fails in control. Examples in the industry include measures of defining a control effective if at a certain level of the hierarchy of control, for example at engineering, and implementation monitoring at above ninety percent. Combined with a matrix, a decision is made that the control is adequate, yet intermittent failure was never measured. Such a system will not uphold good practice and require a more mature control measurement.
- Wanted failure to reside within a designed system and could easily be defined during the early stages of the design. Disappointingly, only some of these failures form part of our risk assessment process and are mostly neglected for many reasons. A good example would be the design of a humble hook on a shaft conveyance. The control function provides a stable and effective measure of connecting the hoist rope to the conveyance attachment. It will function in this state for many years, but it must fail to provide a safe condition when challenged under specific conditions. When the winder goes into an overwind or under wind condition and any conveyances go through all

other safety devices and fail to stop the conveyance, the last resort is to ensure the rope detaches before being pulled into the shelve wheels. The spectacle plate will force the humble hook to open and detach the rope, allowing the conveyance to drop into the jack catches safely in recovery.

Level of protection assurance is another technique used to determine quantitative control effectiveness. On its own, it may not be the best control effectiveness or performance measurement technique, but combined with the bow tie analysis, it can discriminate between controls.

- Control of similar design and intent are aggregated into control families.
- Systematically select controls that require a different level of assurance.
- Following a designated criteria to isolate the most critical controls on which other controls depend.
- Other controls are subject to the effectiveness of a critical control; if it fails, the rest of the controls also fail.

The defence lines designed within the level of protection assurance process will allow excellent quantifiable response points on the event pathway, which influence risk velocity or measure the impact on reducing risk velocity. The approach is fundamental to a trigger action response plan.

Principles of consequence control have similar effectiveness criteria but require a measure during and after events, which must be simulated without the real-time event. The definition and principle of risk treatment as described in the international guidelines for risk management have selection options reflected in sub-clauses, and references are made to control effectiveness and change the magnitude of the consequence. If the safety objective of any organisation relates to “zero harm”, then consequences should receive preference over

any other control that engages with likelihood. At this point, traditional risk control collapses for several reasons, which include aspects such as:

- Organisations are more authentic in performing well with tangible risk, mainly because the impact or consequences are apparent and simplistic, whereas intangible risk requires more detailed analysis.
- Most risk assessments currently in existence are merely a population of the team members' knowledge, subjective to their opinion. Thus, controls and their effectiveness are highly subjective when considering human factors.
- Numerous organisations have implemented a diverse control effectiveness technique, which they use in conjunction with the Bow Tie Analysis. However, it is never used as a selection criterion for determining a control's criticality.
- Threatening and of grave concern is the evasiveness of not using escalation factors as integral to the effectiveness criteria. Because of this neglect, the subsequent development of critical control regimes becomes a more administrative function and supervisory burden.

For too many years, organisations have done risk assessments and maintained a system of review and mounting new controls. Limited emphasis was placed on evolving effective control strategies, defying the release mechanism and where controls ought to be as close as possible to the risk source. The tendency had been to reduce the likelihood of the risk event. Naturally, the brain takes the easy way out or the rosier part of the process. Intentions must change, and consequence control effectiveness should be quantified in relation to the magnitude of the risk source, and for that, we require a comprehensive process. Many advisors and software suppliers have drafted templates with idealistic perspectives of risk assessments, however, with little if any constructive contribution to control effectiveness

analysis. The biased proneness of consultants who complicate controls and exploit the confines of company systems has become the norm of the day, while informed risk managers should brand them.

Likelihood and consequence control effectiveness have common ground, which should be contemplated in distinct selection categories. Deserting the opportunity to use the different control dimensions will sustain a fallacy of traditional control effectiveness being suitable. Areas that should be targeted for effectiveness per dimension include:

- Scenarios to shift the control framework on the timeline closer towards the threat and as close as possible to the release mechanisms of a trigger event, and ultimately controls well into the pre-condition phase.
- Similar shift on the timeline towards the subsequent risk event control, mitigating the downstream events.
- Exploiting the prospects of using 3-D principles by shifting the control analysis from a single characteristic to that of all consequence categories, revealing the total consequence domain. Thus, control encompasses critical aspects of effectiveness that reveal the spectrum of impact, i.e., health, safety, financial, production, etc. This activity may challenge the existing use of the Bow Tie Analysis programmes as very few of the software allow for the integration of control frameworks—an area where Excel is the worst to be used.
- Evolve effectiveness within the hierarchy of supervision and management, and detail measures lowered to the worker or task level.
- Escalation factors that defeat the control objectives have their own controls and effectiveness measures for mitigating barriers.

The criteria to measure control response resides in the design of the control and its objectives. The ability of a control to function under normal and abnormal conditions will reflect in the efficacy of managing the magnitude, frequency, and velocity of the encounter. Theoretically, it makes good sense, but in the hands of the operator, it appears to be complex and unattainable. Historical controls were developed haphazardly as risks arose and fires flared up. A significantly more practical and eligible approach would be a methodology founded on the stated timeline dimensions of control. The risk of a moving conveyor belt can illustrate the dimensional approach to control design in the context of defined effectiveness criteria.

Segmentation - Populate the controls in silos of specific functions.

- Guarding on a conveyor belt is a single preventive control unit.
- Position indicator reflecting the position of the guard (closed or open mode) reporting to a control room is a single monitoring unit.
- An alarm that the guard is opened while the conveyor is moving is a single first response unit.
- The guard and conveyor power supply interlock is a single first response control unit.
- A proximity device that will trip the conveyor power supply when a person comes within the danger zone during belt maintenance or training will be a single first response unit.
- A single first response unit is an automated mechanical interlock that will prevent the runback of a tail or drive pulley during gravity imbalances.
- A single emergency response unit, acting upon the first response failures, automates the release or take-up of the belt tensioner in the event of a person being pulled into a belt.

Structural dimensions—Define control objectives specific to each of the individual release mechanisms that will impede, reduce, or terminate the energy flow in a quantifiable way.

- Guard: Fail to prevent several revolving part release mechanisms.
- Position indicator: Fail on bad instrumentation detection system.
- Alarm: Fail on mechanical functionality. To monitor effectiveness, it must be tested manually and with noise instruments at levels and distances.
- Proximity: Fail on the accumulation of dust on the sensors.
- Mechanical interlock: Fail on exceeding structural integrity in abnormal overload conditions.
- Belt tensioner: Release tension to a limited distance from take-up, and inclined systems will remain under gravity tension.

Simulation – Utilise two- or three-dimensional simulation software programmes to test scenarios of control response before implementation.

- Position control objects at design positions, such as the rip detectors, belt alignment switches, and pull wires, in relation to the installation height and the conveyor belt's entire length.
- Activate technological systems to control the different scenarios, such as interlocking devices from a control room or in a loco.
- Apply human activities to normal and abnormal conditions (pedestrians, maintenance, operational functionality testing in motion, inspections, etc.)
- Quantify the magnitude of the risk release before and after control unit activation.

Quantify the five effectiveness measurements – diligence, dependability, reliability, survivability, and accessibility.

- Define high control reliability confidence intervals representing actual test results for the significance level.
- Critical controls can confidently be defined based on quantifiable data as controls with an automated function that has a higher effectiveness rating and imitates a simulation confidence rating of more than 95% or a significance level of 0.05.
- Having simulated information available for the entire life cycle of the control.

In summary, employing these principles to rigid controls requires a resilient process. Education on the control subject has become necessary for understanding controls' dimensions and functional capacity. The challenge remains for organisations to design a control framework integrated with actual work activities in an understandable manner for the rainbow workers. Admittedly, progress has been made over the past few years, and a few organisations have altered their appetite to show due care.

Capturing rigid control structures is essential to progressing in our journey towards resiliency. Organisations will have to provide more resources to perform risk research and, where necessary, support and use educational institution initiatives. With today’s technology, we cannot continue to base our major risk control effort on the input of a single “subject matter specialist; it is just not enough.

Qualification and quantification of the risk source (for cradle to grave) remains the most critical element, specifying suitable and sufficient lifecycle controls. These controls should be captured within real-time event scenario simulations. Using factual research data to verify effectiveness and preventing subjectivity or misperceptions are imperative. Imitate

controls that will reduce impact at source release point, at every change in magnitude, and throughout the lifecycle.

Key risk indicators

The basis of success is measuring performance against a specific standard, the way we truly manage risk relative to risk management. The standard is as important as the performance criteria. Understanding the hazard and risk sources provides information on what to measure, how to measure, and how to compare to established best practices. Essential information to measure risk performance should at least have the following in common:

- This was a pre-event energy-control stage, during which the energy and risk source were still stable and suitable for business use.
- The means by which the risk source manifests itself in the workplace and which mechanism will discharge it in a specific direction.
- Critical is the speed and magnitude of deliverance from the point of non-return up to the target of harm, loss, or impact on objectives.
- During the stable phase to the point of loss, a risk source will undergo numerous transfer stages, metaphoric changes, and yield reflectors of failures. The amount of energy that must be released or forces which must be applied to produce the change in a defined state per unit of time and that can be validated simultaneously.

In the event of a risk source such as a primary crusher, one would seek information to measure the performance of the crusher rather than the reasons for breakdowns or accidents. By analysing the performance, a list of energy sources will reveal each with its function, and each provides a stable state, controlled state, and uncontrolled state. The latter does not reflect a state where controls have failed; it demonstrates the state where the energy is of such

a magnitude and speed of release that the capacity of control parameters has been bridged. These phases become essential for setting up key performance areas, for example, the electrical current used by the crusher against any sudden increase or decrease, the amount of interaction with people outside of the crusher, or the number of times a person attempts to enter the crusher for whatever reason and entering under a stable or unstable state. The key performance areas are dismantled to actual data comparison, where measurement becomes qualitative for the quantity of the forces involved and the expected quality, which provides the capacity of control, which is, in principle, the critical risk performance indicator.

Understanding how to measure risk performance requires a matured risk management system where the terminology has already changed from numbers to big data, from engineering controls to artificial intelligence. Any operation that monitors critical controls by application has a long road ahead. Asking key questions during a visible felt leadership session detaches from the objective of monitoring critical risk performance. Automatic monitoring regimes can track energy, forces, movement and change, producing a more extensive accuracy base for controls to manage out-of-specification indicators effectively. Artificial intelligence takes over high-risk assignments where big data can be used to manipulate self-control under a controlled environment. Machinery such as a primary crusher should not require a person to operate or come to immediate proximity, and if necessary, will close access automatically, warn and stop all energy of forces in time that cannot be overridden by any other system, except the crusher control system itself. Thus, the machine determines the safe state and not the person.

Utilising the best practice as an indicator might not be the best practice, and the same goes for legislation, which carries the burden of being the minimum requirement. Defining the pre-event state will provide the standard of a controlled state within the design parameters. The area of monitoring is established, as well as criteria to measure against.

Transformers are used in all mining operations and pose a significant risk of losing power to a plant and an explosion. Time and money went into prevention measures, procured and employed following insurance and legal audits. We must accept that the recommendations were based on either a past event or a perception of best practices within the field of knowledge. Key risk indicators must focus on the early stage of an event, thus the pre-condition state and, in the case of a transformer, the insulation and cooling design criteria, not if a flash plate was installed between transformers. Forces influencing the dielectric strength can be measured in velocity (the speed of breakdown in voltage rating) and quantified (for example, 150 kV/cm) to provide change censoring. On the other end of the event, existing systems measure moisture in the transformer oil tank, not formally, but with an indicator. Apart from the lack of actual data on the amount of moisture, one misses the rapid increase of pressure inside the tank because of the moisture, and the pressure causes the explosion. The question remains: what is the best practice, the design state, or the moisture?

The closer we shift our critical indicators to the point where the risk source is released, where it starts to drift or change in features, such as velocity, the more effective we will be in our prevention strategies, and the less resources will be spent on mitigating strategies. Managers must have a strong belief in the assurance that monitoring systems generate sufficient information that supports the correctness of their decisions with no uncertainty. Very few monitoring systems in the mining industry consider confidence levels to define achievements. Operators of mines should pay attention to the use of confidence levels and the advantage of using a specific quantity of data to verify control efficacy in response. Risk managers of the future will design key risk indicators with 95% confidence levels, and management should be able to analyse the deviations.

Correctness and suitability of the measure implicate inevitable features that should be considered. The risk indicator structure will comprise confidence samples of a defined level

of accuracy, have a specific degree of acceptable variability and be suitable for the organisation's size. Control effectiveness is therefore affected by the measurement variabilities or possible sample error. Thus, if a controlling owner takes a sample of compliance during a physical inspection or from a control response data system and finds that 90% of workers comply with isolation and lockout procedures, they can confidently conclude that between 95% and 85% of the total of employees will show compliance. The correctness is determined by a 5% variable or error margin.

Managers can no longer accept the 80/20 Pareto Principle; it is not a suitable mathematical law, but it is noteworthy that it is a straightforward outcome without the precision of the sample. It is cluttered with variabilities and, when defined, will aggregate homogeneous units of risk indicators with designated sample sizes. Occupational hygienists have used this for years when sampling airborne pollutants and noise exposures. Translating the same principles into other risk sources with more variables is challenging. In doing so, one may encounter the measure's complexity. The monitoring regime must be designed to exclude random samples or, in practice, inspections or management interactions once a week. It dissolves the current system of critical control verification through inspections and observation conducted by managers, and the sample will not survive the requirement.

Another consideration for a more statistical control effectiveness measure is the data analysis methodology. Suppose the decision is to develop a descriptive statistical analysis of compliance to a standard. In that case, appearances of frequencies and deviations from a mean will suffice, and any number of observations will do. However, more complex data is necessary when it is essential to determine multiple deterioration causes, covariance for causes having the same trend, or log-linear analysis for cause relationships. What does this mean in practice? Quantifiable risk criteria will produce a measure of deviation from a practice that defines the likelihood of an event and, with a defined accuracy level, will outline

the consequence of a breach. Risk assessment maturity will increase as confidence levels of control effectiveness are quantified. Key risk indicators will provide accurate data for early warning systems that proactively stop or deflect an event to a wanted impact state.

A double-deck shaft conveyance at a mine takes thirty persons per deck. The numbers are limited by a count control turnstile at the shift's start and end. Tradition has it that at the end of the shift, as many as possible will get into the conveyance; we all want to get to the surface as soon as possible, especially if there are multiple shafts to get out from. One day, the turnstile is defective, and standard load counting occurs. The employees crowd before the conveyance to enter, and the onsetter cannot control the push from the rear. He battled to close the door, but it did close in the end, bowing into the compartment with the cage door interlock intact and working. The conveyance leaves the station, and the unexpected happens. Because of the excessive number of persons in the bottom deck of the conveyance, the door caught onto the penthouse above the station, opening the door, and four persons fell down the shaft.

History does not predict, it repeats. A cage door makes people inside feel safe; they cannot see the danger outside, a false sense of safety. If the door fails, it is not about the number of employees who enter the conveyance; it is the fault of the authority, managers, and engineers who designed, approved and commissioned it. No, it was the fault of reckless people who became irrational in their decisions. The last person who got onto the conveyance did not do the headcount, was unaware of the numbers and even more recklessly climbed into the conveyance, squeezing himself so that the door could be closed, lucky not to have his fingers caught in the door's runner. Unfortunately, the door was ripped out of its runners when it passed the penthouse above the station, and a few people fell down the shaft before the conveyance could be stopped in midshaft. A tragedy never seen before and erratic in

aftermath. We could have prevented the tragedy if we had key risk indicators with detective, predictive and surveillance monitoring rules.

If industry accident statistic, which are seemingly declining or trending to be lower, causes a mindset of being safe, then managers must reconsider; it is not a reflection of being safe; it shows history, not the future. If we do not understand the human nature of risk, we are articulating history to repeat. Standards, procedures, and engineering specifications are all needed. Still, they are as good as the mathematical modelling created to understand the variables of human nature that must deal with them seconds before the tragedy.

Bow Tie Analysis

Risk management is about coordinating activities and directing related controls concerning identified risks. Managing risk involves fundamental decisions based on sound risk evaluation, analysis, and good corporate governance principles, producing the company's risk appetite. A designated methodology exists for every risk management process within the risk management structure, from assurance, scope and context, assessment, and control response, ending with monitoring and review systems. The industry was known for having reasonably suitable systems in place for all the phases of risk management except the control and monitoring part. In pursuing a solution for the lack of control management, the industry embarked on a practice developed in the early 1970s that displays fundamentals of the traditional fault tree analysis and event tree analysis. The bow tie analysis technique has since evolved into a well-defined threat control evaluation and barrier analysis technique.

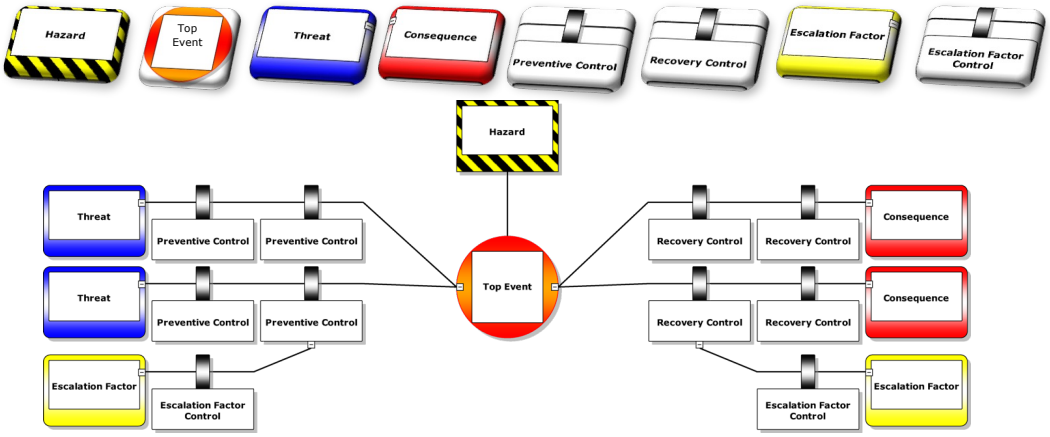

Figure 3: Bow Tie Analysis terminology

Characteristically of the industry, a common approach was established, taking cognisance of what was already done in the petrochemical and chemical industries; both had many years of experience with the technique and were showing the results. After several stakeholder consultations, the International Council on Mining and Metals (ICMM) issued a Critical Control Management Implementation Guide. The focus is not on reproducing the guideline but on implementing it. Validation of the guideline refers to a definite mining industry phenomenon. It implies a psychological effect formulated in 1886 by German psychologist Wilhelm Wundt, which concludes the systematic adjustment of objectives. The imitated effect was to follow the prescribed objectives of the bow tie analysis technique without being side-tracked by the appearance of the critical control guideline. Unfortunately, the objectives were modified, with reasoning to suit the anticipated rapid reduction in fatality rates. A short-term solution dominated the long-term sustainable result. Subjectively, the industry uses bow tie analysis merely to identify critical controls, not following the due process of barrier analysis and advanced control management. Integral to the study was the level of protection assurance, which was never explored and a forgotten principle of a critical factor to the governance of risk, emphasising psychological loss.

The proof of the embedded phenomenon lies within our actions in the thunderstruck upshot and confusion after a significant event when helicopters land and disgruntled

employees or communities block entrances. The mistake was at our doorstep; the industry had a well-defined programme and was on a soundtrack in mid-2011 when the guideline was introduced. Along came the digression from the original objectives, the critical controls and a monitoring system. A matured company had set the pace for development; less matured companies got entangled in the process and gasped for air using uninformed specialists. They lost the plot by fabricating and decentralising an unfounded system that formulated a basic set of verification questions deriving from remarkably ingenuous Excel spreadsheets.

To substantiate the notion, we must understand the mistakes management or executives make in risk management, as explained by Nassim N. Taleb et al. (2009). We are indebted to look into the mirror, compare the objectives, and act according to the deviation from the image. Herewith, I provide a summary of the relationship between the mistakes and the current application of the bow tie analysis.

- We predict future events from a baseline risk assessment, do a bow tie analysis, establish a fabricated control framework with specifications, and live under the fallacy that we have proven capacity to manage the event.
- We use past accident causal analysis, statistics, and trends to estimate the effectiveness of controls and possible likelihood of events and are convinced that we manage the risk.
- We cannot differentiate between advice on what to do and what not to do.
- We use statistical methodologies to inflict decisions based on defined predisposition risk parameters.
- We developed a system to calculate human error, close the gap with automated means, and abandon the psychology behind the error.

- Our profit forecast is exceptional; however, it provides little leeway to manage risk variation. The market thrives on profit but also reacts violently to major risk events, affecting shareholders.

In summary, the industry is very well positioned to identify significant exposures to low-probability, high-impact events. It is prepared to spend time and effort managing critical controls, saving costs and shareholder infliction. Advice to use more engineering controls instead of curing the industry's psychological problems created a gap yet to be filled.

We must acknowledge that risk management is not accident investigation and that accident investigation does not stop or prevent accidents. It is the management of risk that contracts the anticipation, deterrence, prevention, and mitigation of the impact of unacceptable risk. In other words, taking risks on calculative pre-set criteria aligned with the company's risk appetite.

All mining companies have a formal risk management policy that deals with risk, qualitatively or quantitatively, at different management levels. Some work from a corporate enterprise risk management system to a middle management level to a worker involvement level, and several work on a three-tier process while others work on a four-tier process. The number of tiers does not make it more effective. The effectiveness complements the interaction between the layers, regardless of the number, and the flow of information and risk-based knowledge.

Baseline and issue-based risk assessments have become outdated in depicting history; very few have revealed new risks other than the norm. The so-called high risks have remained the same over decades, changed irregularly to suit the month's flavour, and are deceptively affected by accidents. What happens gets recorded, and the industry relies primarily on recorded consequences to determine what should be deemed high risks. Every new event gives the impression that the controls cannot mitigate or deal with the

consequences. Bow tie analysis, on the other hand, lends itself to scenario setting. It has provided numerous new events never recorded before, revealing a suite of absent or misplaced controls in the control structure. Therefore, understanding the framework in which bow tie analysis is done becomes critical to the effectiveness of the outcome.

To comprehend the methodology, one must understand the different languages and philosophies used for the bow tie analysis. It is not a risk assessment or investigation and not a problem-solving technique. The analysis cannot weigh one risk against another in deciding which one is more important to manage than another, nor can it force a decision that one control is more effective than others; it cannot eradicate the risk. It is more about a suite of controls managed according to pre-determined criteria that make the risk acceptable to do our work. It will also show the vulnerability of risk owners.

Appropriately, risk assessment produces a list of risks evaluated on a matrix to set priorities for managing them. The proper way to manage these risks derives from the bow tie analysis, which provides the specific suit of controls to manage a particular threat or outcome, producing those controls critical to the management of systems and physical activities or the monitoring thereof.

Information gathering for a bow tie analysis is as vital as any other risk management activity, so the issue-based risk assessment in the form of a lifecycle risk assessment is required. This ensures that the hazard is revealed in its complete form from the cradle to the grave, with total exposure to management. During this phase, a lifecycle map is drawn, which depicts the metaphoric changes of the hazard related to magnitude, interface with other hazards, external forces, drifting of the hazard, increase in release velocity and lastly, the mechanism that will release the energy of concern at a point of non-return where failed controls can be exposed. The valuable information is plotted on multiple event timelines, having only one hazard with various outcomes. This timeline would serve the purpose of

identifying the point where control has been lost, also called the Top Event of the anticipated bow tie analysis.

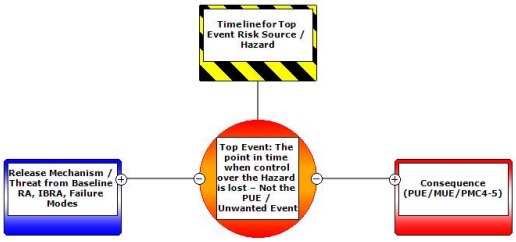

Figure 4: Top Event

Matured bow tie analysis has top events closer to the hazard, and less matured programmes will have the top event either unwanted or as a consequence. For example, gravitational force on the pit wall is a hazard in an open pit mining operation. Matured companies will have 'driving forces exceeding resisting forces' as a top event, whereas less matured companies will use 'slope failure' as a top event. Ill maturity is reflected when the 'inundation of people from a slope failure' is used as the top event.

The missed opportunity is that the control framework will be plotted differently. Preventive controls become mitigating controls and vice versa, and a simple example is when an earth leakage protection system is plotted as a preventive control for electrical shock, where any person with limited knowledge of electricity will advise that the earth leakage is activated after the flow of current between the source and earth, thus a mitigating control. Therefore, the positioning of the top event is the most critical factor of the bow tie analysis and ensures the control framework can be evaluated effectively.

Hazard	Resilient	Pro-Active	Compliant	Re-active	Basic
Hanging wall	Driving forces exceeding existing forces	Changes in hydraulic forces / Increase in stress fields	Loss of cohesion	Uncontrolled fall of ground	Fall of ground, fatalities, loss of production
Flammable gas	Flammable gas ahead of cutting	Explosive atmosphere	Ignition source in contact with flammable gas	Uncontrolled release of flammable gas	Gas explosion, production loss, damage to equipment
Tailing dam wall	Change to the undrained shear strength of the encrusted tailings	Change in the water table position between the zone of saturation and the zone of aeration	Increase in Phreatic Surface (Tailings) - Pore water pressure under atmospheric conditions (pressure head is zero)	Overflow of tailings	Dam wall failure, environmental pollution
Trackless mobile equipment	Inability to operate equipment under normal neurological conditions	Deteriorating integrity of brake system	Inadvertent movement	Loss control over	Collisions, overturning, production loss
Structures	Increase in the rate of deformation	Loss of tensile strength	Loss of structural integrity	Uncontrolled failure of structure	People trapped under structure, loss of equipment

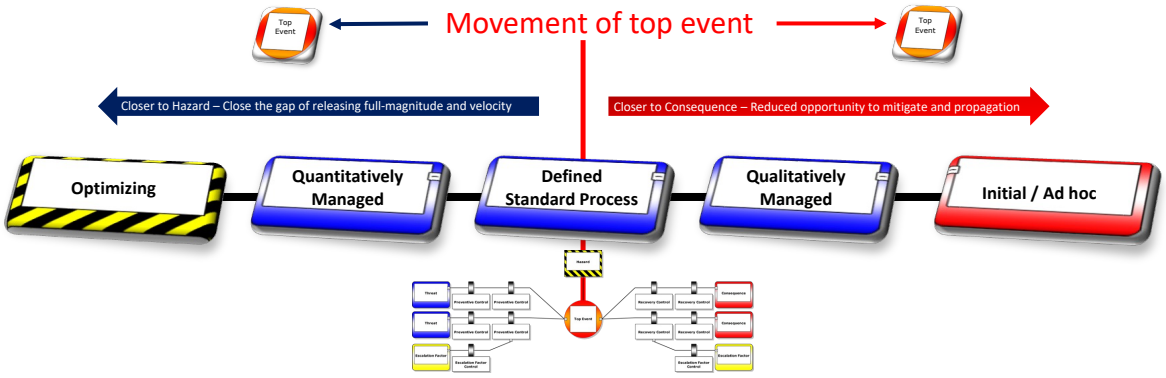

Figure 5: Shift of Top Event Maturity

In recognition of matured systems, we must look in more detail at how the top event of a bow tie can shift on the timeline guided by a specific objective. As mentioned, the matured bow tie analysis will have the correct top event; however, the lifecycle risk assessment has indicated that the control framework needs to be improved to manage the event's pre-conditions or downstream outcomes. It may become necessary to conduct multiple bow ties for the same hazard. Furthermore, the bow tie may extend into another dimension of risk, from the material hazard to a financial risk source. In essence, for understanding, the bow tie analysis starts with a parent bow tie and is broken down into smaller yet mature child bow ties. These smaller bow ties move left and right on the event timeline or back and forth on risk categories, having one aspect in common: they can be linked or chained into a bow tie family. Various software programs are designed with the capabilities to secure the different top event families, control families, activity families, etc. and link them to accident investigation patterns or level of assurance event lines. The explanation is a sample of a cube that contains all the relevant information about one hazard, from cradle to grave, highlighting control effectiveness and the vulnerability of the risk owner to the significant event.

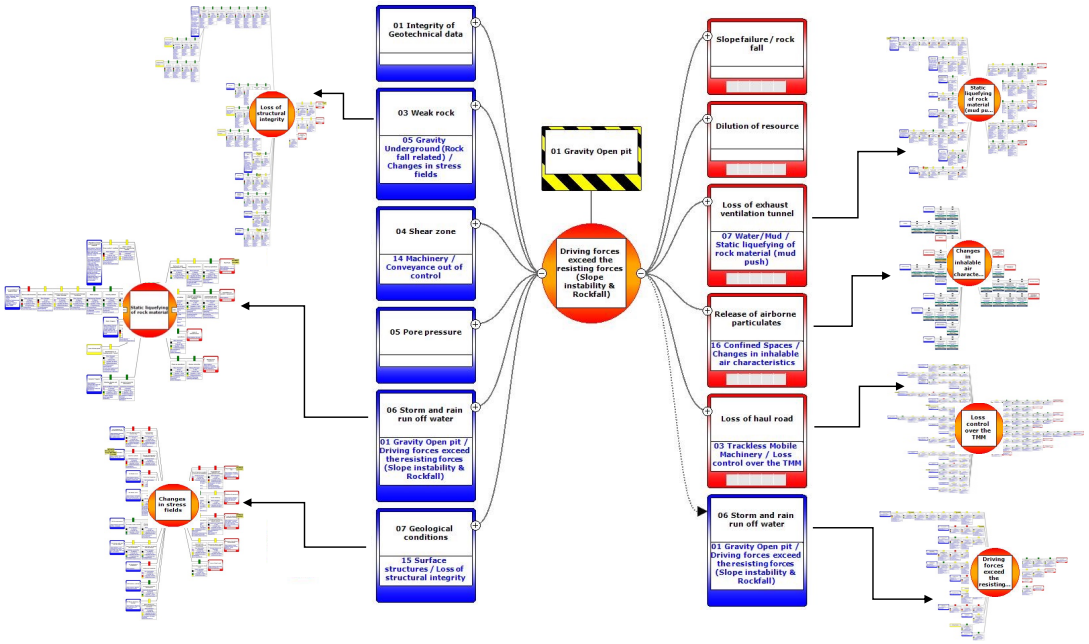

Figure 6: Bow Tie Analysis Family Diagram

A bow tie diagram analyses a specific section of a longer causal chain. The diagram focuses on the crucial phase that leads to an accident. Although the diagram is usually enough to capture all critical factors that need to be considered, sometimes an issue is so complex and far-reaching that we need to look further back. Software programs can chain bow-tie diagrams together to extend the reach when needed.

A factual example of misunderstanding the concept of multiple bow ties can be explained using a transformer explosion timeline developed by professional engineers. What followed next were the considerations in the build-up to the top event and the subsequent outflow of dense confusion, the repulse drives to comprehend the objective of a top event, and, for some, the state of mental uncertainty.

- The oil in a transformer has three essential functions: it maintains electric fields, cools heated electrical components and infuses the paper in the holding tank.
- According to research documents and qualified standards, a dielectric is a medium or substance, in this case, transformer oil, that transmits electric force

without conduction. This point became a critical matter on the timeline, verifying where the oil had been compromised, conveying a condition conducive to an internal arc. Any control in a bow tie should be measurable, for this purpose, the dielectric strength. The breakdown voltage represents a measurement that signifies the ability of the transformer oil to withstand electrical stress without breaking down. The industry standard for new transformer oil is a minimum breakdown voltage of 30 kV (kilovolts) per millimetre.

- Transformers that use oil have two more dielectric materials: paper (on the walls and windings) and/or paint on the windings. The bow tie analysis uses the same three elements during LOPA (level of protection assurance).
- They understood dielectric strength, which directed the discussion towards the causes of the breakdown, which included the operating temperature, increased pressure inside the transformer, moisture when the oil was contaminated by particulate matter, and the formation of gases inside the transformer.
- With conducive conditions, an extremely rapid release of energy takes place in the form of an electrical arc. The arc will cause vaporisation of the transformer oil and ionise the oil vapour. The vapour in the form of gas bubbles and the surrounding oil rapidly increases static pressure inside the transformer tank, resulting in the tank structure's violent failure. During the failure, oil mist is expelled under the pressure and, if ignited, results in a massive explosion.
- Although high operating temperature contributes to the breakdown of dialectic material, it is very often the cause of the explosion.

- Looking at the oil, it seems that contaminants were a major contributor to a few events noted in the industry. Contaminants are represented by moisture, impurities during filling, bubbling with top filling, and arcing.
- The gases released include several combustible gases, such as methane, hydrogen, ethane, ethylene, and acetylene. All were identified as the release mechanism for the previous transformer explosion.
- Combining the arch, which generates explosive mixtures of gas released into the atmosphere during the rupture of the holding tank, effectively describes the initiation of an explanation.
- Finally, up the desk was the elastic and plastic deformation on the holding tank steel structure affected by increased and decreased pressure without an explosion or release. Over time, this can degrade the pressure rating of the holding tank.

From the description of the event above, it was apparent that the early stage of the event is initiated at the point where the “breakdown" occurs. While the arc contains high energy in the form of thermal energy and radiated photonic energy (affecting the cooling properties), it is not the leading cause of the explosion but rather to be noted as an escalation factor, similar to the gas volume and oxygen gap above the oil level. The formation of the water, acids and sludge inside the holding tank and windings is after top event factors and should be discarded for now. They should be noted as an escalation of the impairment of the cooling and insulation breakdown controls.

Over and above the guidance and repeated cautioning of the deviation from the objectives of a bow tie and the definition of a top event, the team decided that the increase in temperature must be the top event, a professional foul. The aftermath raised questions about missing controls, which are critical to preventing an explosion. The team got together again,

and this time around, they followed the guiding principles and tracked the event with more care. The outcome was multiple top events concerning thermal energy, breakdown in insulation, and then oil; in that sequence, the approach was more sequential, and the discussion concluded.

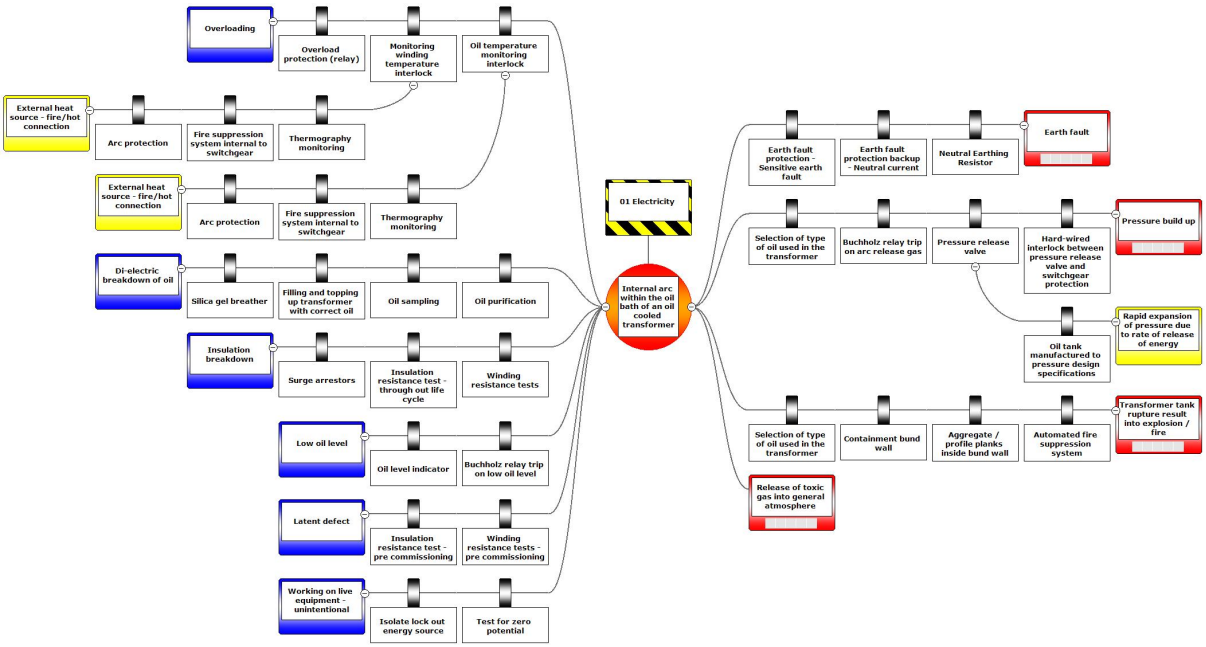

Figure 7: Transformer Explosion

The magnitude of an oil-filled transformer fire or explosion cannot be argued; it will have catastrophic consequences, especially if it happens in a shaft or main intake airway. There should not be a risk appetite for any company accepting oil-filled transformers underground, whichever form of scientific justification is used. One cannot add any control to mitigate the consequence of multiple fatalities and the release of toxic gases. The financial implications of replacing oil transformers cannot supersede a person's life. Equally, one cannot integrate likelihood with probability and consequence. Meaningless is the statement that the likelihood of multiple fatalities has been reduced by monitoring critical controls on the transformer. The likelihood is controlled on the left side of the top event; thus, prevention controls. In contrast, the consequence is controlled on the right-hand side of the top event, therefore mitigating and recovery controls. The only mitigation that could be established with

the five bow ties that followed was to reduce the magnitude through oil removal, not containment, no flash plates and no fire extinguishing mediums.

Before facilitating any bow tie, a few essential decision-making criteria should be defined. These criteria will be used to ensure uniformity, prevent biasedness, and confine subjectivity. Herewith critical areas to be determined through validation, exclusive of uncertainty, which imitates the company risk appetite:

- Preventive control acceptance criteria define what is regarded as a control, such as the use of only an act of a person, a physical object, or a technological system to prevent or monitor the release of the threat or produce the top event.
- Mitigating control acceptance criteria explains at what stage after the top event the control is applied, the sequence of controls, and control trigger points. The requirements should indicate that the consequence cannot be eliminated.

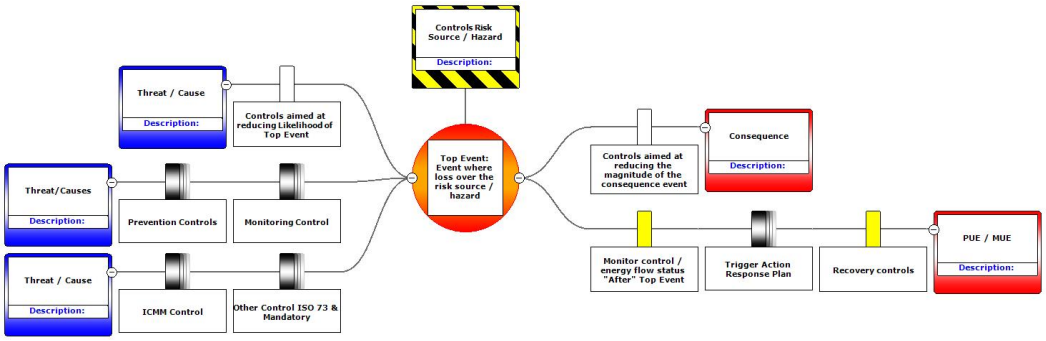

Figure 8: Positioning of controls in a BTA

- Control effectiveness criteria outline qualitative and quantitative specifications for a control's reliability, availability, survivability, dependability, and compatibility. They will include a suite of relevant questions to define objective outcomes regarding failure rates, level of compliance, and impediments.
- The level of protection assurance of controls is an add-on to effectiveness and defines the stability of existing controls in the total control framework of the

bow tie. These quantitative measurement criteria require substantial data with support from a monitoring programme, research, and statistical analysis.

- Escalating factor control acceptance criteria are subject to four basic subordinate criteria. Each defines impedance reasoning for why a control is ineffective and will never be fully effective. The reasoning includes aspects such as natural perils (e.g., rain, mist), critical services (e.g., diesel), inherent mechanical features (e.g., elastic deformation), and human physical or psychological constraints (e.g., circadian rhythm, blindness).
- A control framework depicting the hierarchy and the layers of controls (e.g., supportive, dependent, verification, mandatory). The criteria are linked to the qualitative control effectiveness criteria, with subjectivity on the level of compliance. They should only be used when the monitoring programme has not produced adequate data for the decision criteria to change to a qualitative format.
- The level of competence in management controls defines the minimum expertise required to secure effectiveness. It goes beyond the definition of competence to include risk competence and maturity.
- Monitoring control criteria should detail activities within each control (e.g., calibration, bump start), frequency, and nature of verification. Note that the comment shows that calibration is not a control but a monitoring activity of a control (e.g., a gas monitoring instrument).
- Auditing criteria are characterised by a series of designated questions for field verification and compliance surveys, and a tiered approach is followed.

Once the top event and decision criteria have been secured, the threats are identified. They represent the causes of the top event, simply a step back on the event's timeline. At

what point did the pre-condition transpose into a risk that could result in the top event? Confusion is created by using the word cause in the discussion, and people tend to reflect on accident causes, which include control failures and misleading the threats of a bow tie analysis. Threats do not include any accident caused or any human error. As indicated under the bow tie criteria, human error forms part of the escalation factors. Threats result directly in the top event, singularly and not in combination, and do not cause the consequence directly. In other words, the disposition angle of a waste dump will directly cause the slope to become unstable. The unstable slope loses cohesion and causes the consequences in that sequence. Threats should not be required to happen in combination, and if the top event requires two or more threats to happen concurrently, the top event was incorrectly defined. For example, a fire, as a top event, requires at least three threats, all at the same time. The same can be said about falls on the ground or collisions between vehicles; they all require multiple threats simultaneously and thus disqualify them per definition as a top event. This ill practice is misleading and produces threats such as a lack of support, poor roadway conditions, human error, and failure to lock out.

Threats represent tangible and intangible factors affecting the top event. They necessitate cautious selection with a detailed explanation of boundaries and trigger mechanisms, the frequency of exposure and the relevancy or contribution factor towards the top event. The details are used to determine the commonality between threats, which suggests a possible combination or a split into more different threats. The aggregation or segregation must be done by knowledgeable persons wary of observing when the threat shifts back into a pre-condition or forward on the lime line to an escalation factor. Rain is a natural peril and transmits from a pre-condition to a threat. Rain can also be an escalation factor on either side of the top event, and per definition, it fits all three mentioned factors.

When a top event has occurred, it propagates into multiple consequences, like the unwanted events identified in the risk assessments leading up to the decision to conduct the bow tie. Production loss, injury, property damage and environmental impact have one thing in common: they do not signify a consequence but an outcome of a consequence. The less matured bow ties will have an unwanted fall of ground as a top event and a direct consequence of fatalities. A mature bow tie will have driving forces exceeding existing forces as a top event and fall of the ground due to discriminating against outcomes or sub-consequences.

Hypothetically, consequences postulate opportunity and construct different scenarios evolved from the top event. These scenarios may have happened differently at the organisation, but they allow a chance to evaluate its preparedness to respond and manage such a consequence. Various simulations of scenario events have been done in the industry, and they are widely used to virtually observe a complex risk event and identify additional or unverified consequences. A good indicator of consequences requiring more definition is when the controls become generic in nature and repetitive between consequences. A code of practice or procedure for emergency preparedness and response emerges on multiple consequence path lines because it is generic. However, it needs more details to manage specific properties of event propagation. In practice, such a procedure describes managing an accident scene on site. It might not provide information on recovering a trapped person from a vehicle following a collision. It will lack the specific control to release or demobilise the airbags before starting to use the jaws of life to cut the vehicle and recover the person.

The objective of the bow tie remains to evaluate the effectiveness of controls to manage specific events aggregated after a risk assessment. Dogmatic individuals believe bow ties are conducted to prevent fatalities. They need to redeploy their minds. The objective is to prevent the top event and mitigate the consequences.

Risk management is about controlling risk and positioning progressive barriers to manage a definite event, which makes this possible. A barrier or control can be any measure that acts against some adverse force or intention to maintain a desired state. The effectiveness of barriers becomes the basis of decision-making regarding opportunities deriving from factors revealing the vulnerability of the risk owner. To enable this, a systematic approach is required when populating the barriers.

Firstly, barriers are categorised between those that manage likelihood and others that follow mitigation principles for consequences. This left and right side of the top event is critical to distinguishing between prevention and response. It allows for the identification of definite trigger points and the monitoring of event velocity.

Each barrier has a different objective, which is to ensure the required appetite is met. The objective relates to the threat, the top event, or the consequence. Objectives should be definite, specific, observable, and measurable. It is apparent from the objectives that a procedure or the competency of an operator will not fit into the definition. It must be an act that a person performs using an object or, in specific instances, an instrument to assist with measurement. In other words, an act, object, or technological system.

- An act is defined as the action of the person using skills and knowledge to execute a task. The task should be hands-on activities directed to the objectives of the barrier, such as the test for flammable gas. The barrier is not the completion of the checklist or calibration of the instrument; they form part of the controls that support the effectiveness of the test. The acts of a person include automated sensory performance (intuitive doing), which is rule-based and taught performance practices. A distinction should be made between actual acts of a person using their hands to do the work and where documents or data capturing is the objective, the latter classified as supportive or

verification controls. If all the barriers (checklists, procedures, training) related to an act (gas test) are listed in the same pathway, it creates an illusion that the threat is manageable, whereas all the barriers are, in fact, only one act. Please refrain from using administrative functions as the act. They become supportive and verification controls of the act.

- Objects are used during an act, can operate independently, and may be linked to a monitoring system. The intent is to designate things used to manipulate the flow of energy that have the capacity to monitor change and, where necessary, trigger alarms. Once installed, objects such as interlocking devices (e.g., earth leakage protection) will not require a person to function.
- Technological systems are methods used to monitor barrier status, change, or energy modification so that a person can use the information to take action, or the system can act automatically upon a set trigger parameter. Big data and artificial intelligence are known systems for identifying common human error patterns or flaws and error margins of information used with data analytics to predict effectiveness in managing events.

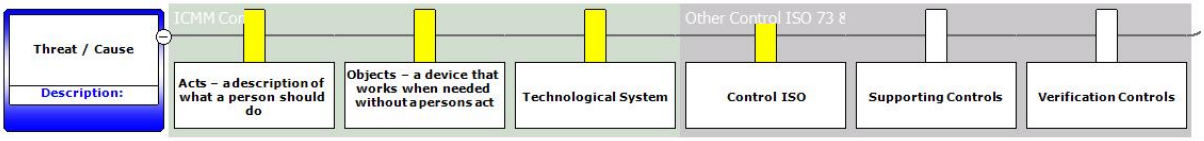

Figure 9: Control families ICMM and ISO defined

Once the barriers have been classified, the next step is to assign supportive controls to enhance the framework's capabilities. The supporting controls consist of dependency and verification controls. Dependency references a control that support the outcome of the act, that it will be performed by a competent person in a manner that produces the specifications of the task, using the correct tools and equipment within a controlled environment. These controls usually include procedures, training, codes, and design criteria. At the same time,

verification controls refer to checklists, maintenance reports, data analysis, and competency assessments. It will verify the availability, survivability, reliability, compatibility, and compliance with the barrier functionality in defining the effectiveness.

The effectiveness of barriers should be assessed by formal evaluation of the variation parameters assigned to the criteria. Indicating a barrier to be 90% effective requires substantial data for such a decision and should not be taken lightly or with subjectivity. Companies that do not make use of designated criteria for levels of effectiveness have flawed the objective of the bow tie analysis technique. Software programs such as BowTieXP have a verification survey or audit module that does the verification in the field, reflects actual effectiveness and does not rely on discriminatory decisions. This was also the point of departure from the technique to become a critical control selection technique instead of remaining a control effectiveness technique.

A matured bow tie will illustrate the effectiveness of all barriers and submissive secondary controls based on a norm which can be verified in-field against a performance specification. Such a survey provides real-time data that feeds the selection automatically. Some barriers are grouped into families with similar objectives and functions and might have similar effectiveness. Validation of barriers encircles the related activities and appraisals. Activities are performed to ensure the act, object, or technological system will function as intended in the design of the control framework.

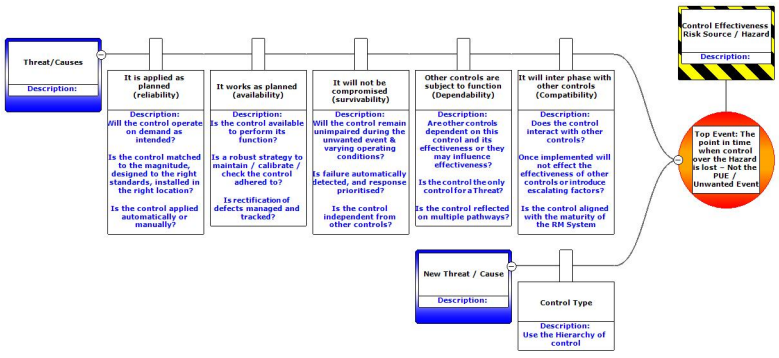

Figure 10: Control Effectiveness Criteria

A bump-start of equipment to verify that zero energy status has been reached would be an example of an activity connected to the test for zero potential. The same can be said for using an object, instrument, or device to determine zero potential in a hydraulic system. Very specific to the barrier and what the objective would be. Appraisals include the requirements to reveal effective performance. The most critical aspects of verification are the questioning in systems, hardware, procedural and legal, competency, maintenance and detection. The performance of each fragment or part of the process is essential, and listing all parts, equipment, substances, and materials in use for the activities or related to the barrier is compulsory. The criticality of the barrier may reside in one part or component. If not correctly identified, the focus shifts to other areas. Criticality is not subjective to a barrier but to the activity or component of part of the equipment. It is not the hydraulic pressure that is critical for a brake system to function effectively. It may be the setting that releases or forces the spring plate into action. Validation thus can pinpoint the crucial part within the control framework with reasonable accuracy.

On the opposite side of effectiveness is the failure rate of barriers, which can be substantiated with monitoring data. The failure rates also represent limitations of barriers and, in some cases, indicate that a barrier does not have the capability to reach its full potential and is subject to escalation factors. Each barrier is assigned to a level of protection capability, thus the independent protection of detecting and preventing the top event or mitigating the consequences. Those which reflect an inability to maintain a parameter of the control function and operating criteria will be selected for assigning escalation factors.

As mentioned earlier, escalation factors have at least four categories related to a barrier. These are the factors that influence the capability to perform to the full and require additional controls to mitigate their impact. Care should be taken that escalation factors do not overlap with treats in the same bow tie. As a threat, rain reduces traction and causes

skidding of a vehicle on a gravel road. However, as an escalation factor, rain minimises the effectiveness of water management controls such as road camber, which aims to divert water to a stormwater drainage system or type of material used for road construction, ensuring proper drainage. Escalation factors inherently comprise the opportunity to improve barriers by design and, therefore, should be enhanced through action management or critical control management.

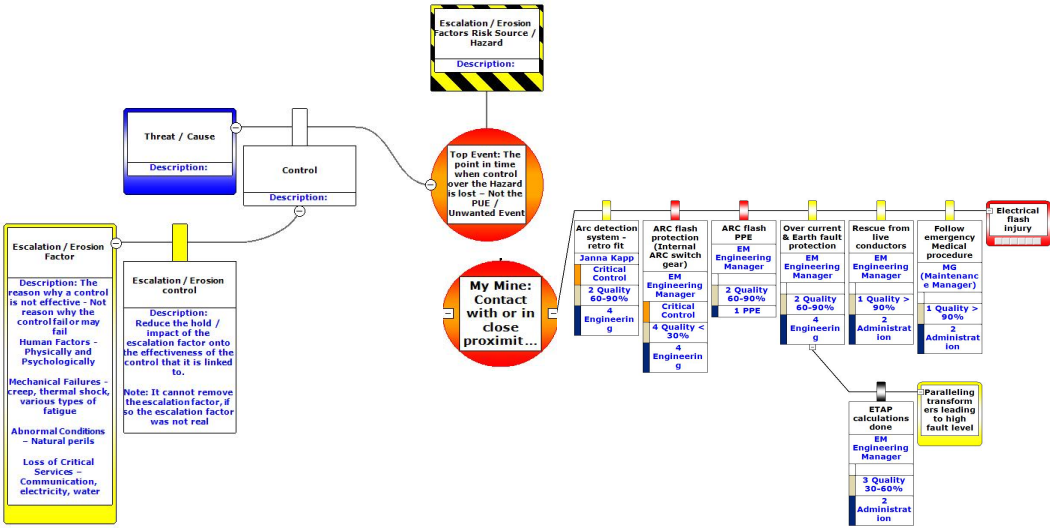

Figure 11: Escalation factor criteria and example

After completing all barriers, with supporting and verification controls, a formal calculation should be made to determine the probability of failure and the maximum reasonable outcome. The successful calculation is subject to the level of protection analysis and the functioning of mitigating controls as intended. The resultant is the vulnerability statement and residual risk requiring contingency plans. Following the calculation, the risk assessment can be updated with the residual risk in the description and risk ratings. The bow tie analysis approach to residual risk prevents predisposition statements and is specific to sequel events.

The result can be influenced perceptibly by controls with a distinctive characteristic of subjectivity, such that other controls will fail if they fail. The indiscriminate breakdown of controls will radically change the outcome, and the event will propagate into a disaster at

high velocity. An add-on advantage of the bow tie analysis is highlighting these controls, categorised as critical controls. They carry a high level of change with quantifiable magnitude, have considerable velocity or rapidness, and have intermediate escalation.

Critical control management

The Romans first used glass as a window. Today, over the many years of evolution, glass still has the same purpose. Although the design changed in an esthetical way, the remaining factors were that they control the exchange of light, airflow, or impact of weather. Glass in its colour and shape donates the attractiveness of a building. The esthetical appearances of the building can rapidly devolve unless maintained, and such a building will be branded as dilapidated very soon. Similarly, there was the opportunity for critical controls, first used in other industries and then converted to a panoramic view through a seemingly small window for the mining industry. The sophisticated appearance was refined with guidelines and well-presented implementation strategies. In theory and practice, the window of opportunity associated with these critical life-saving controls became a broken window in a very short period. What we saw as the best opportunity for drastically improving fatalities was rapidly filled with graffiti of perceptions.

Critical controls are not a new concept. They have affected the food industry since the early 1900s. Leading the way was compelled by exemplars of having pieces of glass identified in baby food at the user's point. It has the potential to close any internationally renowned company within days. Although the frequency of comparable events has drastically reduced over the years, they still materialise.

The graffiti has it that some controls, independently or in combination, will prevent accidents from happening. Indeed, an optimistic way of looking at the impact is only if you understand the concept of critical controls. What went wrong? The objective was to verify if all controls designed and implemented to manage an event's likelihood or mitigate the impact

should such an event occur have been in place. Note the reference to all controls, not a selective few. After that, the effectiveness of each control within its function, concerning interactive controls, is determined, and then action is taken to decrease vulnerability. A holistic view before any attempt is made to select the critical ones. At this point, a matured system can quantifiably indicate the control with the most significant impact of change to the outcome. Simplified, the controls that can prevent the event, or if that is not possible, reduce the consequence to an acceptable level.

Each of the links of a chain is critical. If used to lift an eight-ton ladle filled with molten metal, one might want to signify a few more critical links than others. It might be the link the closest to the heat, the one connected to the shackle, or the one in the middle. Deciding which control is more critical than another should not be done based on the person's perception. The earlier discussion on human error and groupthink philosophies should diminish the way of doing. The layers of protection data are the frame of the window. Having a window that does not fit the frame devastates the system. The industry will have to shift the paradigm to artificial intelligence in one way or another.

Easier said than done. Changing the control definition, design, and surveillance features to sanction data points to measure the impact on a complete event control system might be challenging. From the critical control effectiveness discussion, we now know the expectations of what to monitor. The control performance standard and verification should define the specifications for tracking the use of artificial intelligence. Instead of setting the control reliability to meet a legislative or any other standard, the focus should be on how often the trigger event challenged the individual control and how frequently the control functioned normally, partially, or with total failure.

For example, the industry has used energy isolation and the related lock-out and tag-out processes for over 34 years. Competent artisans who are strictly rule-based follow the

procedure. It has many detective practices and supports a well-documented permit system for the validation of effectiveness. However, every year and more, we have a serious incident involving machinal or electrical equipment. The unfortunate result of largely rules-based systems is that the violations thereof are predominately echoed by severe injury. If the equipment is to be isolated and the tools used to lock out and tag out remain the same, everything will stay the same, people and their behaviour will not change, and future events will recommence. If we want to monitor the actual application of only one aspect, the lock, we must start using smart locks, also called intelligent locks. These pre-programmed devices communicate via a designated SIM card to a control panel, which will inform the user and supervisor of any malpractice or deviation from the programmed norm. Multiple cross-references have been built into the digital locking devices, for example, the isolation plan of each piece of equipment, request and access, anomalies, energy type, mechanism of the lock, validation of positive and negative energy status, etc.

More stable and secure monitoring systems are required to accept an electronic system to gather structured big data for artificial intelligence. Bluetooth, SIM cards, leaky feeders, Wi-Fi, etc., in all or in combination, have their risks, but they should be addressed in that they provide a window of opportunity to improve the existing paper-driven systems.

This brings us to the point of selection: Which control is more critical? A proper definition of each step should support any such programme and not depend on a person's perception, experience, or qualifications.

- Step 1: Complete the risk assessment using a technique to illustrate each control’s associated risks within the lifecycle and the event's timeline. The step should replicate the critical point where the control must be introduced to be effective in function. Failure to locate these critical points results in random

decisions and misleading order of priority. Here, specific well-designed software programs assist in event and control simulation.

- Step 2: Define the control objective, function, and, importantly, dependency on or of other controls. Activities such as equipment calibration to maintain the control status will enhance the decision-making process.
- Step 3: Assign control families. Ensure that interdepended controls are combined into one family and, where possible, have the option of individual selection. Note that these controls might be at an escalation level and significantly impact the upper level of the control.
- Step 4: Establish the reliability of each layer of protection. As the single most crucial element of selection, it is applied to determine measures needed to achieve an acceptable and quantitative risk level for each scenario. Not only are causes and results for a scenario evaluated but also attention is paid to specifying and developing protective measures. Sufficient data should be used to qualitatively decide if a control will function on demand and produce the intended outcome. The point of failure of each layer of control (families of control) and the trigger to activate the next layer of controls should be defined. The control criteria used for each layer of protection form the basis of the control effectiveness monitoring principles.
- Step 5: Select only controls that are engineering in design and application, have an electronic monitoring system, or have the capacity to implement artificial intelligence control regimes.
- Step 6: Define the monitoring structure. Essential elements to consider are the placement of sensors, the type of sensor that will ensure the accuracy of surveillance information, the wanted, discarded or pre-emptive engagements

and the malfunctioning response plan. The monitoring system is interlinked with the layers of protection, its failure and trigger of the next layer. Matured systems will automate these activities and prevent any human interference.

- Step 7: Revisit the vulnerability analysis. This last step requires a back-analysis technique to confirm that the current measurements correlate with the forecasted design data and parameters.

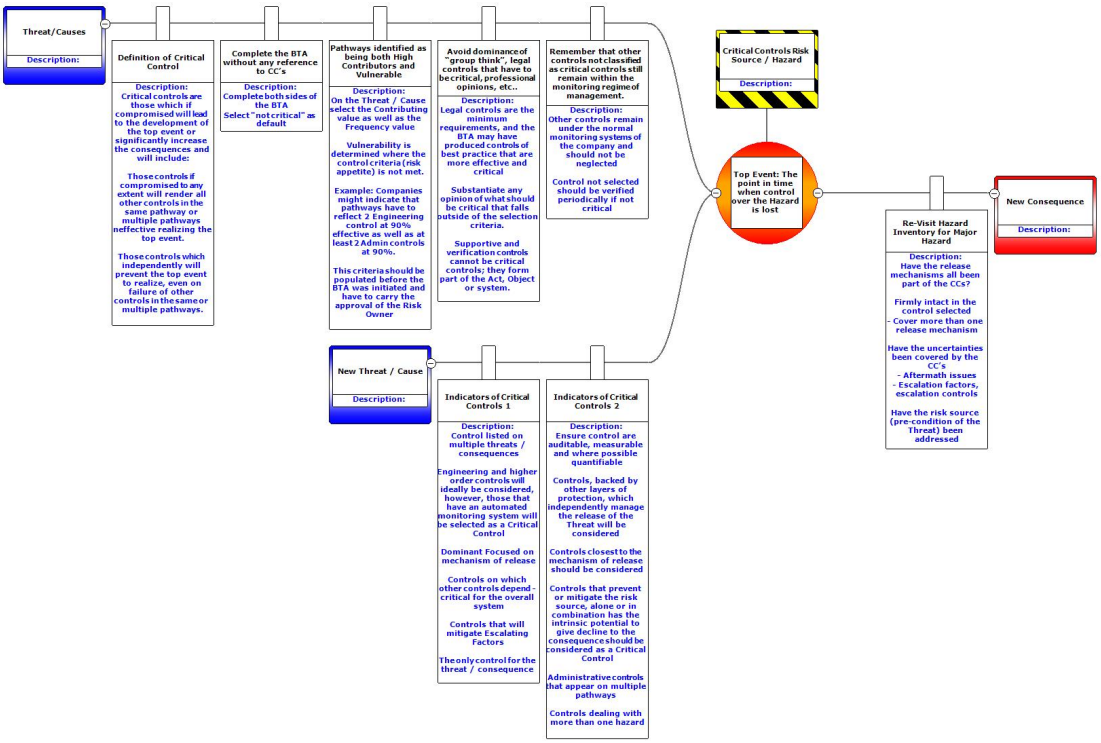

Figure 12: Critical control selection criteria

A few things have been corrected in the past, and we must focus on the selection process's objectives. The facilitator should guide against the following aspects to avoid bias and discrimination between controls.

- Groupthink: Experience presented numerous examples of control selection being manipulated by a group towards the rationale of a person biased towards a specific outcome. Love and beauty belong to the eye of the beholder. Correspondingly, they are the selection of critical controls without guiding policies. Individuals with the authority to negatively influence the critical

control domain can belittle the process. Consensus on critical controls can only be reached with essential reasoning, evaluation, and consequence management. Mostly at risk are the cohesive groups of engineers and managers who have operated in the same environment for many years. There is a notion that occupational hygienists have been part of such a process in the past. They tended to operate within an isolated group of professionals, obtained group leadership within their association, and focused on homogeneous outcomes, all good features of groupthink.

- Priori reasoning: Facilitators must distinguish between a priori assumption and a priori truth. The industry is filled with critical controls, presumably decided upon by experts. However, upon closer scrutiny, they have a diminutive effect on the outcome of an event. Spring-applied hydraulic release brakes on trackless mobile equipment exemplify such a priori. On the other hand, it is a list of critical controls that, without any evidence or experience, are known to, individually in the application, prevent an event from occurring. The disconnecting of a power source by pulling out the cable connection from the switchgear is an example of such a priori.
- Human acts: Guidelines portray an act, object, and technological system approach, but when it comes to the critical controls, the facilitator should guide the assessors that the act does not counter the behaviour of a person and has no relationship. The act as a critical control does not represent a task but a control within a task. Thus, the test for zero potential energy on a capacitor is not a critical task. It is a critical control within the greater task of de-energizing a capacitor.

- Clustering of controls: There is a fine line between dismantling a control into smaller fragments and clustering into larger chunks. A good practice is to start with the fragmentation and then cluster them where objectives overlap. It is essential to show the fragmented option before selection, and it may be that the critical control is one of the smaller fragments and not the total family of controls. Fire suppression on a trackless machine is an excellent example. Critical discussion should start with the design, placement of nozzles, extinguishing medium and quantity, feed line routing, activation process, and covering the entire life cycle of the fire response.
- Terminology: Ensure that the terminology relates to the operator responsible for implementation. Several risk management techniques are complex and filled with technical evidence. It is the facilitator's responsibility to ensure understanding and maintain the integrity of the function. Using terms such as driving forces exceeding exiting forces for the top event of a bow tie ends in confusion and misleading control placement. The operator in the workplace understands the loss of cohesion, which is technically different, but will not affect the preventive and mitigating control selection. Instead, it will better understand where to find preventive critical control.
- Administrative: The practice of having administrative controls as critical controls has the effect of a barking dog. Besides being annoying, it does not prevent a criminal from entering the premises. Equally, an alarm that sounds before a conveyor belt starts is a critical control, so why keep selecting it as critical?
- Behaviour controls: Administrative and personal protective equipment controls rely highly on human behaviour. Good practice will discard them as

critical controls, however, not without considerable dispute. An example of a flash suit for switching can be used. As the lowest effectiveness of all controls, many companies use it as a critical control for electrical hazards. The facilitator should have used the bow tie analysis to show that the control was inadequate and that remote switching should have been implemented. Selecting a critical control to suit the inability to change and improve risk management is not a good practice.

- Habitual decisions: Each person knows how relative values affect work relationships and human actions. Habits resulting in critical controls are dangerous practices comparable to modern operational diseases. Safe declarations and permits to operate are no different from documents that prove the work can continue, with or without the correctness of the tick marks. Over the years, we get operators that obtain a PhD in tick and flick. Facilitators should be able to identify these habitual activities and controls and, without exception, remove them from the decision criteria.
- Mitigating criticality: The principal objective is to prevent the event from happening, yet we find multiple critical controls on the mitigating side and less on the preventive side of some of the bow tie analyses. Self-contained self-rescue devices and refuge bays underground are excellent examples. The amount of capital allocated to fire suppression systems for conveyor belts, rescue equipment, and facilities resides in mitigation. Critical controls cannot be bought; they must be earned.

Managing the critical control monitoring system requires an electronic collaborative system with iterative capabilities. A best practice would be a package deal between risk assessment, monitoring, analysing, and communicating. Bow tie XP software is a package

that provides evaluation and includes layers of protection, quantification of risk levels, monitoring surveys, live and automated information updates, and management actions.

Selection is followed up with control specifications, performance standards, and the verification process. Information for this phase should have been developed and used during the bow tie analysis process. The control functionality defines the owners' roles and responsibilities within the event's overall control framework.

- The competency of the person who must perform activities governed by the control, which may include, among other things, instrument calibration, non-destructive tests, back analysis, observations, and settings.
- The upholding principles ensure that the control remains unimpaired and operational on demand. Reference is made to design principles, certification through inspection authorities, and quality assurance guidelines.
- Control performance measurements include vibration limits, supplier-conducted primary and secondary vehicle brake response tests, and brake temperature limitations with interlocks.
- A response or recovery plan is a trigger mechanism for applying the next control layer. Automatic translation from the first layer of control to the second layer, such as primary brake failure activating the secondary bake system and subsequently retardation to a stop function.
- Features of Key Performance Indicator: Its obligations are before employment of the control, during application, and before discarding or termination. Ensure the alignment of roles and responsibilities with the company's risk appetite. It provides a quantifiable and tangible metric used to measure the effectiveness of the control framework.

- Verification should be based on the quantitative regime established with the key performance indicators. Mainstream measurement includes in-situ monitoring, devolvement, risk velocity acceleration and deceleration rates, escalation rates, control distortion, sensitivity feature movements, and deviant impact. A yes-and-no answer technique generates paperwork with a less-than-useless database, is old faxed-based, and obscures the reliability of the critical control program.

Once completed, a test and validation phase is followed before implementation. Risk modelling and simulation within defined parameter settings are good practices. The realistic and authenticated control response is measured, gaps are identified to optimise the control framework, and lessons learned are closed out before implementation.

Risk response plans

Many risk assessments would have stopped at the point where residual risk had been identified. Based on perception or a lack of understanding, they have concluded that when the risk was ranked once or twice, without and with control measures, they achieved a risk number suitable to determine the risk profile. Such an approach has effectively muted the risk response and contingency plans.

Taking one step back, risk evaluation is defined as comparing the results from the risk analysis with the risk criteria to determine whether the risk is acceptable at a defined magnitude. In submission to the risk appetite, the business or business unit can decide its readiness to bear the risk after risk treatment. Hence, the risk of vulnerability, acceptance, or tolerance would only be determined by considering the response and contingency strategies.

Risk response planning is the process of deducing and iterative measurement. The risk event is evaluated against the risk criteria with its mitigating controls to determine acceptance or tolerance. Suppose the requirements still need to be met. In that case, the procedure is

repeated in the same sequence and continued until it yields successful results or delivers an outcome closer to a desired objective. This process of repeatedly attempting to reduce the magnitude has pushed the mining industry into research programmes and employment of technologically advanced risk control measures. Risk response plans cannot remain stable, stagnant, muted, or placed in hibernation. Monitoring and review of the risk management framework has the function of response and, in best practice, producing a response plan for each contributing factor or agent of the event, and it will support:

- Response to the trigger event in the effort of terminating the release or decreasing the event's velocity and magnitude, effectively managing the likelihood and propagation of the event. The intent is to evaluate the first point of the trigger event as described in the trigger action response plan and measure the capacity of the control to manage the event. An example may be the movement measure at a prism position on an active slope of an open pit mine. The slightest indication of ground movement recorded should initiate a response, and this response should be documented with suggested actions and responsibilities.

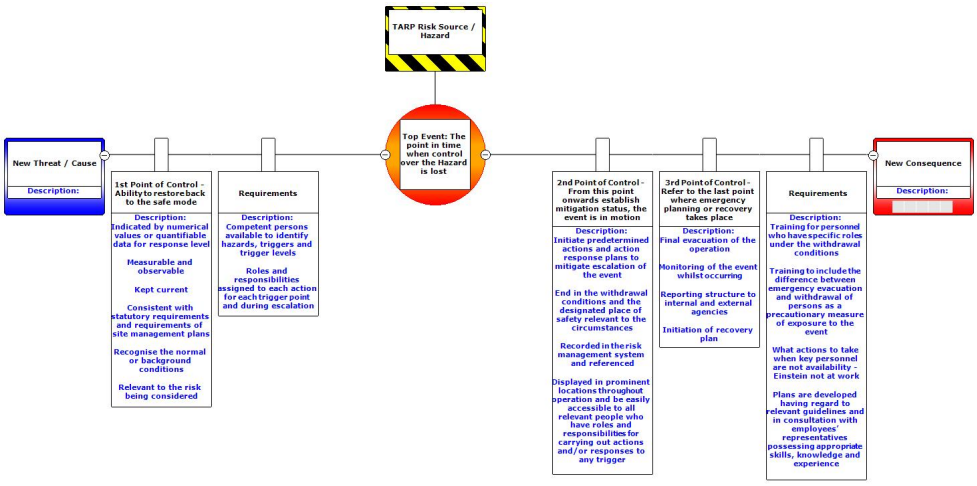

Figure 13: Response plan within the BTA process

- Response to each control capacity within the nature of occurrence, in the sequence of application and on the event timeline. It must embrace responsibility and authority for detailed actions of when to activate the control, like a trigger action response plan. In the above example of slope monitoring, the response will have multiple trigger points with numerous actions before a slope failure. Still, it will also include the actions during and following the slope failure.
- Response to the event if controls have failed under normal and abnormal conditions. The response plan extends to an emergency, recovery, and contingency plan. A multiple bench failure in the example under abnormal conditions may include a mudslide with an inrush of water and losing access to the ramp. Propagation scenarios will test the effectiveness and resilience of the programme.

Contingency plans are like backup plans, and they are designed to address subsequent unforeseen occurrences or surprises during and after a risk event. It outlines the sequence of actions to mitigate the event's impact and restore the former status quo. A best practice would include all the scenarios created during the significant hazard management risk assessment and bow tie analysis. Each scenario will have its response and contingency plan, detailed to appropriate execution once such an event occurs, and importantly, have the following in common.

- Continual effectiveness, efficacy, and efficiency measurement. The intent would be to streamline response actions, eliminate bottlenecks during the response, avoid repetitive activities, and improve resource deployment during the event. Further, to evaluate factors that influence the anticipated outcomes through empirical evidence. Impartial consideration of internal and external

capacity, risk knowledge, varying context, response implementation reliability, resource availability and accessibility.

- Consistent training and education programmes are required for persons who have a role or responsibility in the response plans. Trigger action response plans are integral to the process, and interim change will affect reliability and survivability.
- Consistent, proactive drills and exercises include internal and external affected parties. Interaction with local communities is challenging in nature and subject to consequence and impact assessment. Sensitive information may release pre-event rumours and must be addressed in the response and contingency plans.
- The plan is continually maintained to ensure it remains current with operational demand, change readiness, and liquidity of the business unit.

The ability of an organisation to bounce back into 'business as yesterday' after a disturbing event reflects its resilience. Significant hazards in the mining industry are associated with multiple fatalities. They are extremely disturbing for the industry, the local community, the market, and any other person working in the industry. Resilience has made the sector incredibly strong over time and flexible to adapt. Even though response and contingency plans are generic, the ability to return to the status quo after a disturbing event has shown to be successful.

Assurance auditors verify the existence of response and contingency plans based on evidence. They will assume confirmation of hibernating systems in the absence of actual events. High-risk events should have a direct link to definite response plans; a simulated programme must substantiate the result of the ability to respond effectively. A formal risk assessment that captures information on an Excel spreadsheet or in a disruptive software library is impractical and away from goodness. It must provide credible evidence to show due

care. The matured operations have leapt to generate real-time simulations, virtual interactive educational systems, and immersive environments that produce highly efficient response teams.

Where do we find the trigger points, and how do we define the actions? Opportunity resides within the company's Bow Tie Analysis programme. Including parent bow ties linked to child bow ties allows for movement within the three-dimensional arena of risk management. In other words, a top event of a bow tie produces a consequence with a suit of mitigation controls. Part of the mitigation is the initiation of the response plan. What needs to be added is the rest of the response, the recovery, and the contingency controls. To enable the discovery process, shifting the top event of the bow tie towards the right and along the release timeline past the consequence is necessary. Developing a new bow tie based on the consequence unlocks the direct and latent impact. The control population has been a significant eye-opener, and they lack or are incredibly generic in most instances.

Figure 14: Control and Response points of a BTA

Note that the bow tie requires a particular format for defining the post-consequence impact, hence the comment on the controls. For example, the pit wall slope failure produces a dust cloud directed towards the access road to the local town. Every person travelling through or seeing the dust cloud has their own opinion of what happened at the mine. It might differ from a blasting event to people trapped, a building collapsing into an open pit, etc. Internally, perceptions might also vary from when the crown pillar failed. Should we wait for the control room operator to respond? These different scenarios form the centre of the impact assessment of the newly developed bow tie. An extended bow tie will reveal the realism of the response controls, which must follow the consequences.

Response controls relative to each of the post-event impacts are directed to the magnitude and severity of the event. In some instances, escalation factors might surface, and it is here where contingency plans must be well defined and tested against effectiveness within the bow tie control framework. Response and contingency plans differ from gravity and will not all fall into place at the event's start. Roles and responsibilities to manage critical points of each critical control must be defined and tested, and event drills must be simulated to ensure chronological, timely, and correct execution during the actual event.

Appetite for Risk Culture

Trust grows with cultural evolution, and uncertainty and opacity increase with cultural devolution. The gap between the two forms opportunity, which concedes to measurable outcomes: an increase or decrease of both objects. To understand risk appetite, one must examine the traits that encourage our perception and trust in making these decisions to exploit or revert from risk.

Most importantly, uncertainty has alternative subcategories informed by information. The uncertainty framework consists of natural, data-induced, and randomness.

- Natural uncertainty refers to the inherent variability of diverse information. Therefore, it is impossible to increase or decrease the variability by making more measurements, using a smaller margin of error or using more sophisticated equipment. In practice, critical controls are measured to reflect the resilience of the risk management system. It also positions the system on a maturity level concerning risk culture. In essence, measuring critical control questions by numbers produces compliance status, which fails to measure the control's quality or the system that supports the control. Natural uncertainty requires quantitative and qualitative measurement of information. The latter produces the uncertainty level affecting a person's appetite. It alarms the mind about the trustworthiness of the information, hence the hesitation to act upon risk.
- Data-induced uncertainty is derived from data selection, data cleanliness, variables, and data transformation. Modelling data to stimulate decisions requires computational methodologies with estimated parameters and predictions. Modelling produces information used for critical controls and trigger action response plans. Inaccurate input produces inaccurate output,

similar to parameter setting and estimations. Accurate data output comes at a cost, takes time to gather and becomes more sophisticated and complex the smaller the margin of error. Information exposed to algorithms has the potential of increasing uncertainty because of the simulation outcome, which may not match the prediction of the technical expert. Artificial intelligence or the Internet of Things should be used with the necessary care. It might create a sensitivity towards system evolvement and, conversely, create uncertainty for the user needing to understand the methodology of artificial decisions made on their behalf.

- The randomness of information arises from its independence. Thus, the accuracy of the information cannot be quantified, and the user accepts the imprecision of the data. In practice, we measure critical controls and base our outcomes on a small sample of observations. Managers will use walkabouts, inspections, and observations to verify critical controls, document the outcome and await the dashboard to reflect compliance. The variation of the randomness of the information gathered has unqualified uncertainty attached.

In summary, the information we use to determine risk levels, critical control effectiveness, maturity or any other form of decision influencing risk appetite is subject to uncertainty. The more accurate the information we share with employees having to respond, the more trust will increase. The master of any disaster knows the courts of the day are a culture of denial. Missing, unreliable, conflicting, and confusing information all form the framework of a devolving risk culture.

In risk culture, resilience is about addressing the derivation of threats and triggers while strengthening a system's capabilities and resources to survive risk events and function within a risk framework. The increase in trust is parallel to the decrease in uncertainty,

forming the foundation of a secured risk culture. Trust has its uncertainty and comes with the same information variables already discussed.

One must understand that “trust” is part of the social makeup of the workplace environment, with a few common and key drivers, namely fear, consequence, embarrassment, and retribution. Many attempts over the years have had little to no effect on the “increase of trust” approach to improving safety. The reason is the limited knowledge we have on the subject and the perception of understanding the minds and matters of a safety and risk culture.

Take, for example, the trust someone will place in the hands of a medical doctor without being exposed to any previous medical procedure. To a certain extent, most of the human population is afraid of surgery, over and above the uncertainty of success or failure. The more critical the surgery, the more uncertainty there will be, and the more the person will have to trust the medical practitioner. Only when the person recovers from the anaesthetics will the person realise that the procedure was successful. However, uncertainty will remain until complete recovery. This is totally different and far from comparison to the workplace; employees, supervisors, and managers must trust each other, and this must take place under a high production-pressure environment. Argumentative: you are now the medical doctor and not the patient. Fellow employees trust you, your decisions based on uncertain information affect them. Your risk appetite, maturity to take or avert risk and the capability to act with capacity reflect the risk culture of the company, not just the individual. This shift requires an understanding of how people react under different circumstances.

Building relationships, leadership, accountability, and many older-fashioned and pre-faxed methodologies do not work in today's high-demanding mining milieu. Increasing trust should be addressed more deeply in the culture of risk. The building blocks of trust are fundamentally linked to a person's actions. These actions result from instinct, emotions, and

habits, reserved efficiently or not; they produce conduct affecting people's perceptions. Criminologists and psychologists have commonly referred to the emotions of people as subjects that have to be fed just as the body must be fed. Understanding employees' emotions provides a window into what they experience during the day. Under a highly controlled environment, any step to the left or right has consequences. Feeding emotions is a norm within a social culture, influencing the workplace risk culture.

It is an illusion that existing and historical safety campaigns or behaviour-based safety will increase trust, a fallacy that is not measurable in the context of risk. If this is critical to risk culture, then the controls used to build trust should confirm the critical control standards, such as observable, specific, and measurable.

The enigma of risk culture will remain a topic of deliberation as long as the industry believes that trust can be controlled. In the current dogmatic work ethics and perceptions, I do not see specific substance to the process of building trust. The equilibrium is unstable and inflicted by external factors outside of the control of the authority, who took it upon themselves to build trust between affected parties.

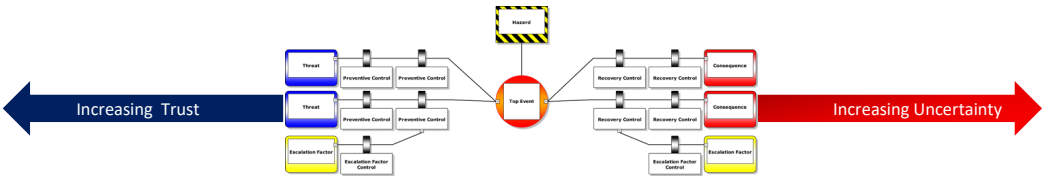

Figure 15: BTA on Trust and Uncertainty

In summary, if trust is earned through hard work, it must be unswervingly reflected on a person or group. Trust becomes variable because the dynamics of trust are disturbed every time a person or group changes, and the change can be as common as transferring a manager or supervisor to another section. The shift in team dynamics, or trust, can increase risk-taking behaviour, bring new habits into the team, and alter the risk appetite of the group.

Understanding risk appetite gives insight into risk culture and the continuous improvement struggle of the industry. Reflecting on a few severe shaft winder and hoisting incidents, one can see a misunderstanding of risk appetite. Stringent rules, checks, and balances are built into the monitoring and action management systems to ensure the safe operation of these equipment. Yet almost every year, there was a significant event, only a few resulting in fatalities. However, when it happens, it has significant repercussions throughout the industry and the public domain. These events occur in South Africa and worldwide in almost every commodity or method: vertical shafts, inclined shafts, declined shafts, and shallow or deep mines. Issues raised are if the industry engineers have an appetite for risk different from production managers, what is the current state of risk appetite, what should the best practice framework comprise, and what does the future risk appetite prototype look like?

Risk appetites are influenced by two factors: risk tolerance and risk capacity. These two factors produce a gap between them, which implies the mitigation gap. Understanding each of these sectors of risk appetite is essential before connecting it to a measurable risk culture.

- Risk appetite refers to the different categories of risk, the amount of risk, and the level of risk a company, a cluster of engineers or a person is willing to take. It also defines who you are and what you want to be. Risk appetite can be expressed in clear statements, stated in a way that supports and protects the achievement of business objectives and agreed to by senior management. In the end, risk appetite is a position adopted by senior management members to pursue their objectives. It is their opinion and point of view, and that is how it should be presented to the rest of the organisation, not as a mandate from the risk manager. The expression of a risk appetite is not a one-size-fits-all exercise. Frameworks can help, but each organisation must lay its path in line

with its risk tolerance and decide how formal, detailed, and mature its risk appetite statement should be.

Essential aspects to consider are how the acceptable levels are determined, the value placed on the related objectives and the trigger point of response. With tangible and material risks, the picture became cloaked. If a conscious decision must be made to continue hoisting with a rope that has a distortion of 10% and an incident happens, the court might find it to be a risky decision and that the company has a low-risk culture, however it was done within the remit of the law. A vehicle has a fuel tank capacity of 80 litres, few will drive until the low-level light comes on and some will refuel when the level reaches the quarter mark. The risk level can be directly connected to a measurable item, be it 10% or 20 litres, and it will trigger a response based on the inherent understanding of the acceptable level by the person or group of people.

- Winding speeds and accelerations hugely differ from winder to winder. A specific winder was installed and could operate safely at a speed of 20 meters per second. However, raising and lowering personnel was limited to 15 meters per second. Variable factors must be considered during the design to determine the actual speed for a designated shaft. This is referred to as risk capacity; otherwise, it is the risk threshold to ensure safe hoisting operations supported with extensive dynamic analysis and tests, including comparisons of legal compliance applicable at the design time.
- The mitigation gap is between the risk appetite (trigger response level) and the risk capacity (threshold). Within this gap, upper and lower limits can be defined and used as key performance indicators to meet objectives.

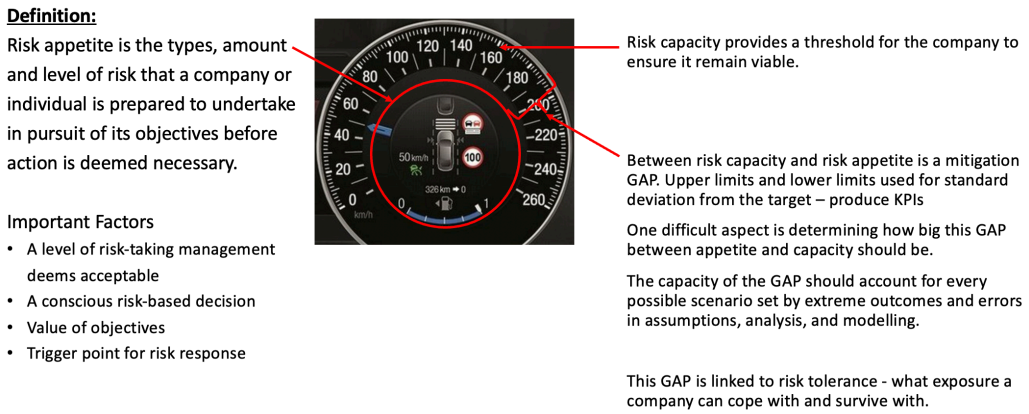

Figure 16: Summary of risk appetite

Safety management was integrated for many years, and risk management still needs clarification. Safety management is a policing practice, i.e. there is a law, standard or guideline that measures compliance and provides a punitive system to rectify. In contrast, risk management aims to manage risk within parameters established within the risk appetite, risk tolerance, and risk capacity of the company. The next generation of risk managers and specialists should acquire the ability to develop risk tolerance statements, risk capacity philosophies and risk response plans within the boundaries of the company's risk appetite statements. It will entail following a baseline risk assessment, and each risk is connected to a defined tolerance level (upper and lower limit), a trigger response to ensure risk mitigation is activated at the right time and, when necessary, the response and contingency plan initiation points. We must note that the existing mining acts and regulations do not allow the full implementation of risk management, as explained. Managers are restricted in numerous ways from pursuing risk. Pedestrian detection and retardation systems are an example of safety management and not risk management.

These challenges experienced by the industry reflect the complexity of risk management and the efficacy of risk appetite initiatives. Risk culture management aims to measure internal performance with external comparison and alignment. Risk appetite, tolerance and response are measured within an information network comprising various

operation levels. Although the perception exists that risk appetite is a driver of risk culture, it is distinctively different. Risk culture is a human issue and denotes how people react or act with risk. To measure these factors, it is essential to consider what influences people's behaviour to risk. It must include aspects such as the echo from the top, how managers perceive and respond to risk, how employees will act accordingly, the risk resources, transparency, and positive recognition.

Although risk maturity and culture are used interchangeably by the industry and some professionals, they essentially designate two detached risk measures. Risk maturity represents a person's capability to perceive, manage, and respond to risk and the readiness to exploit risk in their endeavour for continuous improvement. Numerous models have been developed that exhibit risk maturity in a stairway format. Whereas risk maturity has a bottom level, it should not show an ending, even at the level defined by the industry to be resilient; it will show arrival and fail the principle of continuous improvement. These models are suitable for benchmarking between departments and operations of a company but are limited compared to other companies without the same risk appetite and culture. Efforts have been made to explore opportunities to combine risk maturity and risk culture, and we have noted models developed in the industry, which, in most instances, was a copy from the financial sector. Any attempt to combine the three risk measurement aspects into a one-for-all system should have the capacity and capability to measure the finer detail of each of the subjects. Superficial perception surveys, undirected psychometric tests, 360 ratings and similar questionnaires can deviate from the objective of an integrated model. A proper breakdown of each of the risk traits is required. For example, risk appetite will require the criteria used to determine the risk appetite statement, and for risk maturity, a breakdown of the capability and methodology to identify, understand and manage risk. This detail will provide a well-established framework of measures to classify system opportunities and system devolvement agencies, thus

supporting the continuous improvement strategy. It should now be clear that risk maturity and culture are specific to the nature of operations, the management style, and the operational environment of the organisation, and risk professionals should develop them. Each operation should have an exclusive model aligned with its capabilities. Risk and all its affections are not accessible for any generic approach, and if so, it echoes the maturity of the managers and risk professionals implementing these generic processes.

Robust Risk Management Framework

A good risk register informs corporate decision-making and starts with a risk management framework. The International Standards Organisation (ISO) defines risk framework as consisting of eight principles that guide the characteristics of effective and efficient risk management, and they provide the foundation for management risks. The principles below highlight what risk management ought to provide:

- A defined framework and processes customised and proportionate to the amount and scope of operations.
- Appropriate and suitable participation of stakeholders throughout the risk management function.
- A structured and comprehensive methodology is mandatory for distinct stages in the risk management framework.
- It should be primary and formally incorporated into all operational activities.
- Most importantly, the system anticipates, detects, acknowledges, and responds to changes.
- Inherently, the system should be able to consider and flag any limitations of available information.
- It occupies human and cultural factors that influence any facet of risk decision-making, control framework, or response actions.
- Authenticate continuous improvement principles through well-defined performance measurements and lessons-learned practices.

An effective risk management framework becomes a culture that defines capabilities and practices and integrates strategic decisions to manage risk in creating, preserving, and realising value. The context of a risk management framework is broader and addresses more than internal control, which includes strategy-setting, governance, stakeholder engagement,

and measuring performance. How does the framework look at the upper stratum or executive level, above average operational level? It is divided into three sections:

- The first area is the Risk management structure, which forms the basis of the management approach. This area sets up structures to manage the framework, inform the stakeholders, engage different levels of management and stakeholders, and provide assurance and effective reporting.
- Secondly, the risk management strategy sets the methodologies and aligns them with the company's risk appetite. Philosophies, arrangements for embedding risk management, and policies are translated into objectives that will require result indicators for benchmarking and reporting to the upper stratum.
- The third dimension is the risk management systems, where the actual implementation occurs. The systems provide for designated risk management techniques, protocols, measurements and verification before reporting occurs.

Executives and senior operational managers have different roles. Executives must approve strategic decisions, establish boundaries, and oversee execution. Senior operational managers align strategy, resources, processes, people, reporting, and technology to accomplish their objectives in the interest of established values. The executives define risk parameters, categories, and boundaries. The risk management framework instils a risk discipline throughout management and contributes in three ways: risk management philosophy, risk appetite, and control environment.

- One of the elements of the internal environment is the risk management philosophy, which is the collective beliefs and principles of executives and stakeholders which designate risk culture. It guides how a company considers risk, from identification to mitigation, within everything it does and from

strategy development to day-to-day activities. Many companies have seen the philosophy as the mission statement; however, it should contain more substance than a declaration. It must carry value through the “way we do business”.

A holistic approach to risk management includes the board of directors and other executives, who are not excluded from applying the risk framework. In any event of a change to normal operations in the context of opportunity or risk, the same principles should follow as what is done by the employee using a shovel to clean underneath a conveyor belt. Other significant corporate-initiated changes, such as restructuring, require a formal and systematic risk analysis using the same principles. The industry has seen very few of these high-level risk assessments unless it was done in the aftermath of events such as suicide, post-traumatic stress disorders and related stress illnesses.

Experience indicates unstable philosophies, such as during changes to working hours and shift cycles. Preceding decisions were made by senior management, followed by strategic guidance of the risk assessment directed towards the intended outcome, eradicating stakeholder interest. In doing so, we abolish the values and beliefs of the company, ignoring the time frame of travelling to and back from the workplace at night, limited time with family, hijacking, stray animals on the national roads, and many more elements. When the objectives were not met, the company restructured after a year and suddenly experienced the impact of the original change.

A philosophy is not assigned to an operation; it must be embedded to become culture, from the top down, from the boardroom into the hands and minds of the workers.

- Risk appetite reflects the business risk management philosophy and, in turn, influences the risk culture and operating style. Risk appetite is usually established in a risk appetite statement, which frames the risks the company should accept, the risks it should avoid and the strategic, financial and operating parameters within which the organisation should operate. Risk appetites are a delicate balance. They must be flexible enough to respond to changes in the business environment but not so flexible that their appetite is constantly changing. Altering the appetite frequently will cause a loss of value.
- Five fundamental principles in the control environment support a strong risk governance process. They are the commitment to integrity and ethical values, directors' ascertainment of impartiality and oversight, management's establishment of reporting structures, and the commitment to competent individuals and accountability. A chain is as strong as its weakest link; similarly, a business is as good as its people, and these five principles support the theory.

In summary, applying robust risk management frameworks will strengthen the impact of the governance process on the organisation’s risk culture and, ultimately, the achievement of its business objectives. Notably, the mining industry is filled with procedures and policies, many of which have good intent and are well structured. However, few have proven to take risk management frameworks as an integrated process between all levels, departments and functions. Risk philosophies, appetite and internal control, tend to differ between financial and material risk decisions, matrixes differ, and financial decisions overrule material risk in many ways. This misalignment is natural for the mining industry. As indicated previously, it results from the competency ceiling of the risk specialists in the position of material risk,

their limited exposure to financial risk principles and their lack of integration of the two systems. To explain my viewpoint, stakeholders will prefer a financial manager as a risk manager over a risk specialist as a company's financial manager. The risk management framework requires both and with different roles and responsibilities functioning within an integrated process.

The Future Risk Professional, the Role of a Risk Manager

The traditional risk management processes, which are primarily mandatory, complicated and inflexible, are at a critical point. Listed companies and stakeholders in the financial sector have recognised this change through horizon scanning activities; they have prepared their systems after major economic meltdowns and have set up more robust structures imposed by competent risk owners. However, the mining sector and material risk owners were blindsided. They followed suit with the embarkment on material critical activities with a more complex process. They have this one hurdle to overcome. For many years, a deeply entrenched culture of risk management must be sacrificed, as well as the professionalism of the profession. It all boils down to a directional approach to protect value instead of preventing accidents.

Where previous risk management functions have focused on analysing past events, existing controls, the cost of these controls and the efficiency of the process, a new direction will require a more forward-looking, future control and contingency approach. The primary indicators are graffiti, composed of a rapidly changing world economic environment, war, and natural perils intensifying over a short period. Risk management in the mining sector cannot remain a function of a small group of people doing risk assessments, having a risk profile and a mitigation plan to manage risk independently from the value chain. Protecting the lives of people is as important as protecting the business.

In a world characterised by increasing information technology, which continuously moulds new business strategies, risk management will focus on decisions that enable companies to react and be change-efficient. Identifying change on the horizon differs from identifying possible material events that do not uphold opportunity. Where the primary objective of the traditional baseline or issue-based risk assessments was the identification of loss, the new era requires the identification of opportunities—not opportunities to improve

existing controls of change systems but opportunities to exploit or manage the expected change.

Present risk managers who believe that digitisation and automation are the change from a physically documented driven system to a digitally driven one will soon find themselves in the dark. Future risk managers develop and implement digital enable systems that transform information within a risk framework of decision. The future use of algorithms will assist the risk owner with options for risk decisions, and proactive, responsive systems will be able to automate decisions if mitigation measures start to fail. Regulatory and shareholder pressure will remain the same, and an unstable trust relationship will always exist between the workforce, management and the shareholders. Every mining industry fatality has shown the existing systems' cracks. Until the day that the regulator and risk owners acknowledge that risk management cannot be written with the blood of the injured, dismay will prevail.

The first significant change on the horizon is the status of the risk manager. The regulators must replace the safety officer and chief safety officer with a risk officer and risk manager, followed by the required competency. The evolution of recruited employees to become safety officers produced dried fruit. Everyone can identify hazards and pass the buck to the supervisor to rectify the problem, and in so doing, does not accept responsibility or consequence. The industry has already taken the first step of duplicating the work of a safety officer through the implementation of verification owners for critical controls, line managers and supervisors.

The future risk officer will have the skills to provide consultation and advice services. The challenge of the composition of the new risk officer is the enablement of the correct skill set, which might include the deepening of existing skills whilst obtaining new skills. Therefore, the position should engage with authoritative bodies such as the Institute of Risk

Management and carry competencies prescribed by these institutions. Affiliation to these institutions provides access to developing risk information and to become a partner in the transition towards a digital, inventive and agile world.

Hitherto, then, the traditional school stands alone, with fluctuating shades of opinion, having a view that both safety officers and the regulator have the potential to change the world of fatalities. Statistical analysis, as a body of evidence, codes and consequences, has confirmed it not to be. The risk function must have a range of multiskilled professionals in the rapidly moving world, along with the uncertainty of risk and impact.

- Strong emphasis to include a clear and specific mental apprehension and digital affinity.
- Technical expertise in a designated element of risk management, which might include the use of artificial intelligence, augmentation, modelling, and simulation. Awareness of internationally accepted standards in risk management, including any associated or succeeding documents, and ability to implement the contained principles where practicable.
- Abreast of technological advances, cyber risk and threats.
- Transparent, confident and clear communicator using risk information as the core negotiating factor.
- Inherently has the curiosity to dispute the value of change and related opportunities.
- Ability to secure systems for digitisation, automation, data exploration, and modelling philosophies. This will include the skills for data science and the capability to exploit risk virtual reality software.

- With the number of natural perils materialising into disasters with devastating impacts on people and the economies of countries and industries, a need will arise for expertise and specialists in this field.
- The executive and board-level risk function will require the skills to apprehend the principles and structures of risk management. It must change from a reporting and compliance function to a performance function.
- Professionals are to observe all relevant laws and regulatory authorities' requirements, as well as mandatory codes of practice and conduct within their jurisdiction. They are working within the spirit of the law.

Companies that want to survive the onslaught of future risk should develop forceful risk functions, continuously monitoring the risk function's skill set to manage new and emerging risks. They should also appoint risk managers who act with skill, care, diligence, fidelity, honesty and prudentialism.

There is no doubt that future risk will shape the future risk professional. Trends, speculation, perception, and expertise form a good moonshot that provides light into the dark future, a future filled with material risk rather than financial risk. Investors are increasingly applying factors to consider a company's social responsibility and a country's social stability. Focus has changed to how companies govern their responsibility within the labour-sending areas, their international influence on environmental impacts and strategies to uplift cultural well-being with growth opportunities. The gradual increase of geopolitical uncertainty and biodiversity threats, both distressing global dependability and compatibility, cannot be neglected. The impact of widespread war will be felt by future generations for decades, along with the current epochal effects on biodiversity. The future risk professional must accept that past impact on water, air, soil, and nature because whichever event becomes the nightmare of the future is a pre-condition to be managed. One constant remained throughout the years of

risk management: the health and safety risks to a person. The future cannot do away with this most significant risk. Companies that use persons to perform hands-on tasks, who must take actions affecting others, and who employ equipment in any format will be responsible for managing the health and safety risks accompanying the input and output of their activities. It does not matter what the future holds for us; health and safety risks will remain significant, requiring risk professionals to equip themselves with competencies to integrate employee protection systems into the overall risk management strategy.

With this in the background, the next generation of risk managers will have a diverse assemblage of risks to manage and must admit that the function will change from prevention to mitigation. With the explosion of populations, the previous and current generations have come a long way in causing the existing global risks, and the impact must be turned on. Scientific research and future studies will convert horsepower to brainpower for the next level of risk managers.

In conclusion to the future risk managers, I want to assign an enigma to risk for them to resolve in preparation for future challenges: Apocalyptical risk event philosophies will impede advocated theories, illuminating factual results of controls failing at the hand of psychology emanated from humanity.

References

Brandon H Chen. (2022), *A Design of a Digital Lockout Tagout System with Machine Learning*, A Thesis presented to the Faculty of California Polytechnic State University, San Luis Obispo.

Dionne G. (2013) Risk management: *History, definition and critique*, Canada Research Chair in Risk Management, HEC Montréal, CIRRELT and CIRPÉE, Canada.

Douglas J., Anderson G.E. and Committee of Sponsoring Organizations of the Treadway Commission (2015). Leveraging Across the Three Lines of Defense, The Institute of Internal Auditors.

Gerald J.S. Wilde (1998) Risk Homeostasis Theory: *An Overview, Injury Prevention,* 4(2):89-91, DOI:10.1136/IP.4.2.89, Source PubMed, Queen's University.

Governance Institute of Australia (December 2020), Online, *Future of the risk management professional*, (viewed 2024) https://governanceinstitute.com.au/app/uploads/2023/11/govinst_fotrmp_nov2020-1.pdf.

Hering-VPT (10 March 2022); *Understanding Dielectric Strength in Transformers*, (Viewed 2024) https://www.hering-vpt.com/article/understanding-dielectric-strength-in-transformers/#:~:text=Dielectric%20strength%20is%20measured%20by,kV%20(kilovolts)%20per%20millimeter.

Israel, Glenn D. (1992) Sampling the Evidence of Extension Program Impact. *Program Evaluation and Organizational Development*, IFAS, University of Florida. PEOD-5.

Middle Ages - Nordan Symposia. https://www.nordan.daynal.org/wiki/Middle_Ages

Nassim N. Taleb, Danile G. Goldstein, and Mark W. Sptznagel. (2009). *The Six Mistakes Executives Make in Risk Management*. Harvard Business Review 87(10):123-123.

Philosophical realism. https://en-academic.com/dic.nsf/enwiki/635916

Rasika A. Mathias, Wenqing Fu, Joshua M. Akey, Hannah C. Ainsworth, Dara G. Torgerson, Ingo Ruczinski, Susan Sergeant, Kathleen C. Barnes, Floyd H. Chilton. *Adaptive Evolution of the FADS Gene Cluster within Africa*. PLoS ONE, 2012; 7 (9): e44926 DOI: 10.1371/journal.pone.0044926.

Risk culture - IRM PROTIVITI | PDF. https://es.slideshare.net/SimoneLucaGiargia/risk-culture-irm-protiviti

Risk culture a5_web15_oct_2012 | PDF. https://www.slideshare.net/KymJaeger/risk-culture-a5web15oct2012

Rittenberg, L. Martens, F. and Committee of Sponsoring Organizations of the Treadway Commission (January 2012), Enterprise Risk Management: Understanding and Communicating Risk Appetite, American Institute of Certified Public Accountants.

The Relationship between Internal Controls, ERM, and the Business Model | Enterprise Risk Management Initiative. https://erm.ncsu.edu/library/article/the-relationship-between-internal-controls-erm-and-the-business-model

Ulrich Beck. (September 2017), The Metamorphosis of the World: *How Climate Change is Transforming Our Concept of the World*, American Journal of Sociology 123(2):631-633.

Epilogue

The book title captures the intriguing scenarios of risk management in the mining industry, amplifying the groundbreaking progress made by fellow risk managers and production managers during my career.

The book covers concrete risk management principles with several practical examples from the industry. It can potentially upset some readers who are either dismayed, ignorant or trapped in the ‘resistance to accept the truth’ age. The intent was to highlight key aspects and learned lessons and exemplify them with years of production and consultation experience. A turning point in my career was when I realised the vast number of eccentric viewpoints, interpretations and strongholds developed around individuals on their high horses. The profession is at a threshold point where directives should come from professional risk managers who have the qualifications to advise, support the highest ethical and professional standards, and take every opportunity to improve their professional capability.

AC van der Vyver

+27798722978